2018-03

Law enforcements dilemma: fighting 21st century encrypted communications with 20th century legislation

Owen, Robyn J.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LAW ENFORCEMENT'S DILEMMA: FIGHTING 21ST CENTURY ENCRYPTED COMMUNICATIONS WITH 20TH CENTURY LEGISLATION

by

Robyn J. Owen

March 2018

Thesis Advisor: Erik Dahl
Second Reader: Christopher Bellavita

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2018	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE LAW ENFORCEMENT'S DILEMMA: FIGHTING 21ST CENTURY ENCRYPTED COMMUNICATIONS WITH 20TH CENTURY LEGISLATION			**5. FUNDING NUMBERS**
6. AUTHOR(S) Robyn J. Owen			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

This thesis explores the issue law enforcement has been confronting since the Edward Snowden leaks prompted technology companies to design their communication devices with enhanced encryption. As a result of these modifications, many investigations have been stymied because providers claim that they can no longer furnish law enforcement with device and communication content, even when so ordered by the court. Device designers and communication providers claim that enhanced encryption is intended to protect individual privacy and corporate intellectual property. However, these changes have resulted in providing criminals and terrorists alike with avenues to communicate anonymously and out of law enforcement's reach. A significant issue is that legislation has not kept pace with emerging communication platforms. The Policy Analysis method was employed to explore potential solutions to this issue, culminating with the conclusion that the problem requires a two-pronged approach to address both data in motion, and data at rest. Data in motion refers to communications in real time, and it should be addressed by installing spyware to capture the content. Data at rest refers to stored content, and it should be addressed by the use of split-key encryption. Both methods would require amending current statutes or drafting entirely new legislation to cover existing and future communication platforms.

14. SUBJECT TERMS enhanced encryption, electronic communications, law enforcement			**15. NUMBER OF PAGES** 117
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

LAW ENFORCEMENT'S DILEMMA: FIGHTING 21ST CENTURY ENCRYPTED COMMUNICATIONS WITH 20TH CENTURY LEGISLATION

Robyn J. Owen
Intelligence Research Specialist, Department of Homeland Security,
Homeland Security Investigations, Tucson, Arizona
B.S., College of Notre Dame, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2018**

Approved by: Erik Dahl
Thesis Advisor

Christopher Bellavita
Second Reader

Erik Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis explores the issue law enforcement has been confronting since the Edward Snowden leaks prompted technology companies to design their communication devices with enhanced encryption. As a result of these modifications, many investigations have been stymied because providers claim that they can no longer furnish law enforcement with device and communication content, even when so ordered by the court. Device designers and communication providers claim that enhanced encryption is intended to protect individual privacy and corporate intellectual property. However, these changes have resulted in providing criminals and terrorists alike with avenues to communicate anonymously and out of law enforcement's reach. A significant issue is that legislation has not kept pace with emerging communication platforms. The Policy Analysis method was employed to explore potential solutions to this issue, culminating with the conclusion that the problem requires a two-pronged approach to address both data in motion, and data at rest. Data in motion refers to communications in real-time, and it should be addressed by installing spyware to capture the content. Data at rest refers to stored content, and it should be addressed by the use of split-key encryption. Both methods would require amending current statutes or drafting entirely new legislation to cover existing and future communication platforms.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AWA	All Writs Act
CALEA	Communications Assistance for Law Enforcement Act
DHS	Department of Homeland Security
DOD	Department of Defense
ECPA	Electronic Communications Privacy Act of 1986
FBI	Federal Bureau of Investigation
IoT	Internet of Things
NSA	National Security Agency
VoIP	Voice over Internet Protocol

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

An investigative tool often exploited by law enforcement to further investigations is analyzing target communications. These communications may be derived from telephone devices or various electronic means, and in some cases the investigations may be extremely time-sensitive, such as kidnapping or terrorism cases. However, law enforcement is currently encountering difficulties with providers or device creators who claim that they are unable to comply with court orders in providing the requested information.[1] The main issue is that the devices are being intentionally engineered to safeguard personal privacy and corporate intellectual property.[2] Engineers are designing evermore enhanced encryption that their own companies assert they cannot bypass.[3]

For many years law enforcement has relied on its ability to intercept and exploit subject communications in furtherance of investigations. The Communications Assistance for Law Enforcement Act (CALEA), which was passed in 1994, requires providers to furnish law enforcement with the means to intercept traditional telephone and Voice over Internet Protocol (VoIP) communications.[4] However, many new forms of communication continue to emerge that do not fall under the umbrella of CALEA, such as Skype peer-to-peer messaging, gaming consoles, social media, and BlackBerry

[1] John L. Potapchuk, "A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act," *Boston College Law Review* 57, no. 4 (2016): 1404–1405.

[2] Ibid.

[3] Ibid., 1405; "Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants," *Washington Post*, September 18, 2014, https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.0192bb7759ae.

[4] "Communications Assistance for Law Enforcement Act," Federal Communications Commission, February 10, 2011, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

encrypted email.[5] In addition, providers and electronic device designers, such as Apple and Google have begun engineering their products with enhanced encryption.[6]

Even when served with proper legal process, some companies claim that they cannot comply with court orders and provide law enforcement with the requested information or assistance, because they are unable to bypass the encryption designed by their own engineers.[7] Targets of investigation are drawn to communication methods that allow them to operate anonymously. Enhanced encryption techniques and the lack of adequate legislation to cover these emerging forms of communications hamper law enforcement's ability to conduct investigations.[8]

A significant gap exists between what law enforcement believes is reasonable access to information it has been able to obtain since CALEA was enacted, albeit in a different format, and what privacy experts and technology companies perceive as continued government overreach. Following the Edward Snowden leaks, technology companies began to enhance encryption to safeguard their intellectual property and customer privacy.[9] Privacy experts assert that providing access to electronic devices by introducing vulnerabilities to assist law enforcement would unduly increase the risk to individuals and businesses alike.[10]

Government officials have offered suggestions for how CALEA could be amended to mitigate the deficiencies, but it is not known if sufficient legislative support

---

[5] Christa M. Hibbard, "Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance," *Federal Communications Law Journal* 64, no. 2, art 5 (2012): 372–373, http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1617&context=fclj,

[6] Potapchuk, "A Second Bite at the Apple," 1403.

[7] Ibid.

[8] "Encryption and Cyber Security for Mobile Electronic Communication Devices," Federal Bureau of Investigation, April 29, 2015, https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.

[9] Craig Timberg, "Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police," *Washington Post*, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.7afa491b5834.

[10] Harold Abelson et al., *Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications* (Cambridge, MA: MIT Computer Science & Artificial Intelligence Lab, 2015), 10, https://people.csail.mit.edu/rivest/pubs/AABBx15x.pdf.

exists to make any of these proposals a reality.[11] Privacy experts and technology companies argue against amending CALEA, contending that these emerging forms of communication should not be treated the same as standard voice intercepts, as individuals tend to divulge more private information through these means.[12] In addition, many types of decryption techniques are currently available that could allow law enforcement to continue accessing the information it requires; however, privacy experts and technology companies fiercely oppose these methods.[13] The question this thesis attempts to address is, How can law enforcement access encrypted and emerging electronic communications to further investigations without compromising individual privacy and intellectual property?

The research and analysis for this thesis has culminated in five conclusions. The first conclusion is that newly drafted legislation or legislation amending CALEA is necessary to solve the "Going Dark" issue. The second conclusion is that due to the limitations of existing legislation, the private sector has acted in a manner that constrains law enforcement's authority to conduct legal searches, even when armed with proper legal process.[14] The third conclusion is that prosecutors may inadvertently be doing the agencies they represent and law enforcement in general a disservice by delaying or underreporting wiretap statistics reported to the court. The reported statistics are passed on to Congress, who evaluates them for various purposes, to include assessing the seriousness of the encryption issue.[15] When roughly one-third of the statistics are not reported in a timely manner, or at all, this may prove detrimental to garnering support to

[11] Hibbard, "Wiretapping the Internet," 376.

[12] Ibid., 387.

[13] Kevin Schaul, "Encryption Techniques and the Access They Give," *Washington Post*, April 10, 2015, https://www.washingtonpost.com/apps/g/page/world/encryption-techniques-and-access-they-give/1665/.

[14] "Fourth Amendment," Legal Information Institute, Cornell University Law School, February 5, 2010, https://www.law.cornell.edu/constitution/fourth_amendment; *The Encryption Tightrope: Balancing Americans' Security and Privacy—Hearing: Committee on the Judiciary, House of Representatives*, 114th Cong. 2 (2016), https://judiciary.house.gov/wp-content/uploads/2016/02/114-78_98899.pdf.

[15] "FAQs: Wiretap Reports," United States Courts, accessed August 21, 2017, http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports/faqs-wiretap-reports.

address the encryption problem.[16] The fourth conclusion is that despite protestations by privacy and security experts, it is possible to provide law enforcement with the access to communications it requires, while minimizing the risk to individual privacy and corporate intellectual property. Apple deployed its enhanced encryption following the Edward Snowden leaks.[17] However, the company admits that to its knowledge, its previous encryption and code had not been undermined.[18] This level of encryption provided adequate privacy protections, yet remained accessible to law enforcement with Apple's assistance.[19]

The final conclusion is that out of the six decryption/access techniques analyzed, the two that show the most promise are split-key encryption and the insertion of spyware also known as a State Trojan.[20] Employment of either option would require new or amended legislation. Both decryption/access options have advantages and disadvantages. Access to communications and device content is a complex issue. Perhaps the reason it has been so difficult to overcome is that it has traditionally been approached as a single issue, when in reality it requires a two-pronged approach. When law enforcement has the device in its custody, subsequent to an arrest, search warrant or court order, the focus will likely be on retrieving data at rest. Data at rest refers to all content stored on the device, not ongoing communications in real time.[21] In these instances, split-key encryption seems to be the best option for fulfilling law enforcement's needs while still providing a level of security for individual privacy and corporate intellectual property. As this option

---

[16] "Wiretap Reports," United States Courts, accessed May 10, 2017, http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

[17] Susan Hennessey and Benjamin Wittes, "Apple Is Selling You a Phone, Not Civil Liberties," *Lawfare* (blog), February 18, 2016, https://www.lawfareblog.com/apple-selling-you-phone-not-civil-liberties; Timberg, "Newest Androids."

[18] H.R., *Encryption Tightrope*, 190.

[19] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report* (Manhattan, NY: District Attorney, New York County, 2016), 13, http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

[20] Schaul, "Encryption Techniques"; "Growing Opposition in Germany to New Surveillance Measures," Homeland Security Newswire, June 26, 2017, http://www.homelandsecuritynewswire.com/dr20170626-growing-opposition-in-germany-to-new-surveillance-measures.

[21] Nate Lord, "Data Protection: Data in Transit vs. Data at Rest," *Digital Guardian* (blog), June 13, 2016, https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.

relies on the private sector's assistance, it would likely preserve the integrity of the data, withstand judicial scrutiny and keep governmental costs down.

Conversely, surreptitious monitoring of data in motion, communications occurring in real time, is a valuable tool used by law enforcement engaged in ongoing, long-term investigations. In these instances, the device remains in the hands of the subject, who is unaware of the electronic surveillance.[22] The installation of a State Trojan/spyware may be the most efficient method for law enforcement to monitor communications without having to rely on the private sector for assistance. Although spyware insertion is to date an untested method or at least not widely reported via open sources, it seems to have many advantages. The appropriate response to emerging communication platforms and enhanced encryption by law enforcement and legislators should include innovative techniques, and the insertion of spyware onto a target's device is certainly revolutionary. Therefore, drafting legislation that addresses how law enforcement can obtain both data at rest and data in motion, using the techniques described above, may provide the solutions necessary for these issues.

[22] Lord, "Data Protection."

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis would not have been possible without the unwavering love and support of my husband, John, and my mother, Janet. John was an excellent sounding board for my ideas and afforded me all of the time I needed to work on my thesis, as well as the numerous challenging assignments throughout the past 18 months. He picked up the slack at home so that I did not have to worry about anything. Every quarter when I returned home, I was thrilled to see him waiting for me at the airport. He is my rock and I am grateful for him every day. My mom has always given me unconditional love, and her constant words of encouragement during this program have been invaluable. During the times that I felt out of my depth, John and my mom helped me see the bigger picture so that I could press on and successfully complete this rigorous program. Thank you also to my three furry stress relievers, Keira, Kayleigh and Noel. My kitties were great diversions when I got bogged down and also welcomed me at the door when I returned home.

I would also like to acknowledge Dr. Dahl and Dr. Bellavita for their guidance and support in crafting my thesis. Both were extremely helpful in getting the best work product from me and I appreciated their different perspectives. I truly benefitted from their knowledge and experience and am grateful for their generosity.

Thank you to the outstanding Naval Postgraduate School instructors. I was honored to learn from such a diverse group of experts and am grateful for the knowledge you each imparted. This was truly a memorable experience thanks to each of you.

Thank you to my fellow cohort members. Your friendship and encouragement made this a much richer experience.

Thank you also to my agency management who allowed me to participate in this program and take leave when needed to keep up with my studies.

Thank you, all!

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

An investigative tool often exploited by law enforcement to further investigations is analyzing target communications. These communications may be derived from telephone devices or various electronic means, and in some cases the investigations may be extremely time-sensitive, such as kidnapping or terrorism cases. However, law enforcement is currently encountering difficulties with providers or device creators who claim that they are unable to comply with court orders in providing the requested information.[1] The main issue is that the devices are being intentionally engineered to safeguard personal privacy and corporate intellectual property.[2] Engineers are designing evermore enhanced encryption that their own companies assert they cannot bypass.[3]

A. PROBLEM STATEMENT

For many years law enforcement has relied on its ability to intercept and exploit subject communications in furtherance of investigations. The Communications Assistance for Law Enforcement Act (CALEA), which was passed in 1994, requires providers to furnish law enforcement with the means to intercept traditional telephone and Voice over Internet Protocol (VoIP) communications.[4] However, many new forms of communication continue to emerge that do not fall under the umbrella of CALEA, such as Skype peer-to-peer messaging, gaming consoles, social media, and BlackBerry

[1] John L. Potapchuk, "A Second Bite at the Apple: Federal Courts' Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data Under the All Writs Act," *Boston College Law Review* 57, no. 4 (2016): 1404–1405.

[2] Ibid.

[3] Ibid., 1405; "Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants," *Washington Post*, September 18, 2014, https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.0192bb7759ae.

[4] "Communications Assistance for Law Enforcement Act," Federal Communications Commission, February 10, 2011, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

encrypted email.[5] In addition, providers and electronic device designers, such as Apple and Google have begun engineering their products with enhanced encryption.[6]

Even when served with proper legal process, some companies claim that they cannot comply with court orders and provide law enforcement with the requested information or assistance, because they are unable to bypass the encryption designed by their own engineers.[7] Targets of investigation are drawn to communication methods that allow them to operate anonymously. Enhanced encryption techniques and the lack of adequate legislation to cover these emerging forms of communications hamper law enforcement's ability to conduct investigations.[8]

A significant gap exists between what law enforcement believes is reasonable access to information it has been able to obtain since CALEA was enacted, albeit in a different format, and what privacy experts and technology companies perceive as continued government overreach. Following the Edward Snowden leaks, technology companies began to enhance encryption to safeguard their intellectual property and customer privacy.[9] Privacy experts assert that providing access to electronic devices by introducing vulnerabilities to assist law enforcement would unduly increase the risk to individuals and businesses alike.[10]

Government officials have offered suggestions for how CALEA could be amended to mitigate the deficiencies, but it is not known if sufficient legislative support

---

[5] Christa M. Hibbard, "Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance," *Federal Communications Law Journal* 64, no. 2, art. 2 (2012): 372–373, http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1617&context=fclj.

[6] Potapchuk, "A Second Bite at the Apple," 1403.

[7] Ibid.

[8] "Encryption and Cyber Security for Mobile Electronic Communication Devices," Federal Bureau of Investigation, April 29, 2015, https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.

[9] Craig Timberg, "Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police," *Washington Post*, September 18, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.7afa491b5834.

[10] Harold Abelson et al., *Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications* (Cambridge, MA: MIT Computer Science & Artificial Intelligence Lab, 2015), 10, https://people.csail.mit.edu/rivest/pubs/AABBx15x.pdf.

exists to make any of these proposals a reality.[11] Privacy experts and technology companies argue against amending CALEA, contending that these emerging forms of communication should not be treated the same as standard voice intercepts as individuals tend to divulge more private information through these means.[12] In addition, many types of decryption techniques are currently available that could allow law enforcement to continue accessing the information it requires; however, privacy experts and technology companies fiercely oppose these methods.[13] Technology companies assert that their international sales will suffer if they are forced to weaken their encryption to accommodate law enforcement, and innovation may be stunted.[14] The State Department and the Commerce Department have warned that foreign governments hostile to their own citizens may exploit known vulnerabilities to persecute dissidents.[15]

Technology companies have a part to play in protecting national security, and a safe homeland is beneficial as it provides a stable environment for businesses to continue to prosper.[16] Conversely, law enforcement must recognize that actions by other government entities and their representatives have driven a wedge between it and the private sector, and that introducing vulnerabilities into devices presents risks to citizens and businesses alike.[17] This thesis examines the decryption techniques currently available, as well as proposed legislation, a combination of which may provide a resolution to this problem.

---

[11] Hibbard, "Wiretapping the Internet," 376.

[12] Ibid., 387.

[13] Kevin Schaul, "Encryption Techniques and the Access They Give," *Washington Post*, April 10, 2015, https://www.washingtonpost.com/apps/g/page/world/encryption-techniques-and-access-they-give/1665/.

[14] Kevin Bankston, "It's Time to End the 'Debate' on Encryption Backdoors," Just Security, July 7, 2015, https://www.justsecurity.org/24483/end-debate-encryption-backdoors/; Hibbard, "Wiretapping the Internet," 390.

[15] Hibbard, "Wiretapping the Internet," 391.

[16] Amitai Etzioni, "Apple: Good Business, Poor Citizen?" *Journal of Business Ethics*, May 31, 2016, 8–9.

[17] Timberg, "Newest Androids."

B. RESEARCH QUESTION

How can law enforcement access encrypted and emerging electronic communications to further investigations without compromising individual privacy and intellectual property?

C. LITERATURE REVIEW

This literature review provides an assessment of the most current literature, authored by recognized experts in their respective fields, related to the ongoing debate that places individual privacy rights at odds with national security. The reviewed literature is derived from a variety of sources and includes writings from privacy experts, jurists whose leanings do and do not favor national security interests, academia, federal government websites and professional journals.

This literature review is divided into four sections, followed by a conclusion of the sections, and details opportunities to fill existing research gaps. The first section focuses on privacy, what it means and why it is important. The second section concentrates on security and what individuals may be willing to sacrifice to protect it. The third section discusses civil liberties and the position each side in the debate favors, and the fourth section covers law as it relates to both privacy and security.

1. Privacy

Issues of privacy raise concerns on both sides of the spectrum. In one camp, activists scoff at the idea that privacy should be evenly weighed against security, believing that the scales tend to unjustly tip in favor of security interests.[18] Supporters maintain that privacy's worth decreases as a security threat increases and vice-versa.[19] Daniel J. Solove, a law professor and privacy expert, contends that when it comes to security interests, "What should get weighed is the extent of marginal limitation on the effectiveness of a government information gathering or data mining program by imposing

[18] Daniel J. Solove, "I've Got Nothing to Hide and Other Misunderstandings of Privacy," George Washington University Law School, 761, 763, 772, 2007, http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications.

[19] Ibid., 763.

judicial oversight and minimization procedures."[20] Solove continues, "Only in cases where such procedures will completely impair the government program should the security interest be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one."[21]

Others argue that governmental needs trump an individual's right to protect personal information.[22] The different camps also disagree about the value of and need for privacy. Jurist Richard Posner asserts that, "[W]hen people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."[23] Posner continues, "Much of the demand for privacy, however, concerns discreditable information, often information concerning past or present criminal activity or moral conduct at variance with a person's professed moral standards."[24] Privacy activist Bruce Schneier laments that people often believe the false assumption that those who wish to guard their privacy are merely trying to conceal unscrupulous behavior.[25] Schneier maintains that, "Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."[26] Solove asserts that privacy, although tricky to define, is not relegated to those with criminal intent.[27]

Solove also argues that individual privacy rights benefit society and diminishing these rights has a harmful effect.[28] He further opines that information collection harms

---

[20] Solove, "I've Got Nothing to Hide," 761.

[21] Ibid., 761–762.

[22] Richard Mullender, "Not a Suicide Pact: The Constitution in a Time of Emergency," *Journal of Law and Society* 35, no. 3 (2008): 423.

[23] Solove, "I've Got Nothing to Hide," 751.

[24] Richard A. Posner, "The Right of Privacy," University of Chicago Law School, Chicago Unbound, 399, 1977, http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2803&context=journal_articles.

[25] Bruce Schneier, "Essays: The Eternal Value of Privacy," Schneier on Security, May 18, 2006, https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.

[26] Ibid.

[27] Solove, "I've Got Nothing to Hide," 754–756, 764.

[28] Ibid., 763.

society by causing individuals to self-censor to avoid detection.[29] This leads to inhibited individual behavior, expression and freedom.[30] Law professor Ann Bartow poses the question, "Why is the possibility that a person will be linked to her own volitional words and actions a harm that law should pay attention to?"[31] Bartow continues, "Are not the behaviors that get chilled by a fear of accountability likely to be socially undesirable ones?"[32] Some contend that these harmful effects have not been adequately articulated, which is why tougher legislation has not been enacted to further protect individual privacy.[33] Solove's response to this argument is that, "At the end of the day, privacy is not a horror movie, and demanding more palpable harms will be difficult in many cases."[34] He further states, "Yet there is still a harm worth addressing, even if it is not sensationalistic."[35]

It has also been argued that the government's collection of large data sets and use of computers to examine this information does not violate individual privacy.[36] The stated reasoning is that inanimate objects, such as computers, cannot violate privacy and their use may even protect some individuals' data from ever being reviewed by a human.[37] Solove refutes this claim by asserting that these, "Are problems of information processing, the storage, use, or analysis of data, rather than information collection."[38] Solove contends, "They affect the power relationships between people and the institutions of the modern state."[39] Continuing in this same vein Solove maintains that, "They not only frustrate the individual by creating a sense of helplessness and

---

[29] Solove, "I've Got Nothing to Hide," 758.

[30] Ibid., 758, 765.

[31] Ann Bartow, "A Feeling of Unease about Privacy Law," 57, University of New Hampshire—School of Law, January 1, 2006, http://scholars.unh.edu/cgi/viewcontent.cgi?article=1119&context=law_facpub.

[32] Ibid.

[33] Ibid., 52.

[34] Solove, "I've Got Nothing to Hide," 769.

[35] Ibid.

[36] Ibid., 752.

[37] Ibid.

[38] Ibid., 757.

[39] Ibid.

powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives."[40] An issue also arises if individuals lack the recourse to correct invalid information collected by the government.[41] Further, concrete term limits for data storage do not exist in many situations.[42] If the data is not properly handled, it could be subjected to "secondary use" where it is used for an entirely different purpose than what it was initially collected.[43]

Former Assistant to the Solicitor General Melissa Arbus claims that, "In the wake of September 11, 2001, individuals appear more willing to sacrifice their privacy expectations in order to protect the nation from future terrorist attacks."[44] Examples exist where the general public has accepted that "common good" outweighs privacy: "sobriety checkpoints," "random drug tests of train engineers," "airport passenger screening," and mandatory "smallpox vaccinations."[45] As national security threats persist and technology advancements continue to emerge, it is unlikely that existing privacy protections will remain unchanged.[46]

2. Security

Philosophy instructor Irfan Khawaja asserts that, "Security is the feature of liberty in virtue of which each person's boundaries are safeguarded from external boundary-crossings, be it by criminals, terrorists, wayward police officers, or bureaucrats."[47] Khawaja conjures the words of Alexander Hamilton on the subjects of security and liberty and interprets them thusly: The belief that Americans must sacrifice liberty for

---

[40] Solove, "I've Got Nothing to Hide," 757.

[41] Ibid., 766.

[42] Ibid., 767.

[43] Ibid., 767, 770.

[44] Melissa Arbus, "A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era," *Virginia Law Review* 89, no. 7 (November 2003): 1733–1734.

[45] Etzioni, "Apple: Good Business?" 3.

[46] Arbus, "A Legal U-Turn," 1734.

[47] Irfan Khawaja, "Not a Suicide Pact: The Constitution in a Time of National Emergency," *Dissent Magazine*, 102, 2006, https://www.dissentmagazine.org/wp-content/files_mf/1389818084d8Khawaja.pdf.

security is fallacious, because protecting liberty protects security by default.[48] However, as Solove points out, weighing security concerns against privacy rights generally favors the former, as thwarting additional terrorist attacks remains a priority.[49] Combatting radical extremism requires that law enforcement collect and analyze massive amounts of personal data.[50] Jurist Richard Posner's view is closely aligned with a famous quote attributed to David Hume, an 18th-century philosopher.[51] Hume was quoted as saying, "The safety of the people is the supreme law: All other more special laws are subordinate to it, and dependent on it."[52] Posner contends that in the name of national security, U.S. lawmakers should give the NSA "carte blanche."[53] The prevailing wisdom is that law-abiding citizens have nothing to hide and therefore should not fear or question the government's need to access their data.[54] Supporters question why it matters if the government examines their personal information.[55] If they have not committed a crime then law enforcement will proceed to the next person's information, having not harmed them in the process.[56] In this same vein, the collection of meta-data appears to have a low–level impact on individual privacy, compared to the high impact on national security if a terrorist attack is stopped.[57]

The response to this argument lies in what is known as the "Mosaic Theory."[58] Although the collection of meta-data may appear relatively harmless, this data can be

---

[48] Khawaja, "Not a Suicide Pact," 103.

[49] Solove, "I've Got Nothing to Hide," 753.

[50] Mullender, "Not a Suicide Pact," 423.

[51] Ibid., 422.

[52] David Hume, *An Enquiry Concerning the Principles of Morals* (Salt Lake City, UT: Project Gutenberg, 2010; 1912 reprint of the edition of 1777), Section III of Justice, Part II, https://www.gutenberg.org/files/4320/4320-h/4320-h.htm.

[53] Grant Gross, "Judge: Give NSA Unlimited Access to Digital Data," PCWorld, December 4, 2014, http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html.

[54] Solove, "I've Got Nothing to Hide," 747.

[55] Ibid., 753.

[56] Ibid.

[57] Ibid.

[58] Gabriel R. Schlabach, "Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act," *Stanford Law Review* 67, no. 3 (March 2015): 677.

aggregated and used to forecast potential acts.[59] Attorney Gabriel Schlabach asserts that, "Under this theory, certain types of long-term (or otherwise expansive) surveillance violate a suspect's reasonable expectation of privacy, even when each individual act of surveillance would otherwise pass Fourth Amendment muster, because the government can analyze the information in the aggregate to infer private details about the suspect that no individual member of the public could reasonably discover by observing her for a short time."[60] Emerging technologies may also provide other ways in which aggregated data could be exploited.[61]

Posner also argues that the United States is in a continued state of emergency due to terrorist threats.[62] As a result, he contends that for as long as the country is under threat, the President should be empowered to temporarily discontinue or at least curtail constitutional rights.[63] Those opposed to Posner's stance take issue with his nebulous use of the term emergency.[64] His detractors claim that with Posner's limited definition, the United States could be in a state of emergency for decades, and its citizens subjected to limited rights for the duration.[65] Khawaja likens Posner's views to that of a dictator.[66] Khawaja takes exception with these opinions and declares, "If the safety of the people is the supreme law, it is hard to see how that safety can be preserved in a regime of the sort that Posner envisions, where in fact nothing is ever safe."[67] West Point instructor Aaron Brantly contends that, "Terrorism remains a problem and a challenge to liberal democracy, but undermining the digital security of society without improving the

[59] Solove, "I've Got Nothing to Hide," 766.

[60] Schlabach, "Privacy in the Cloud," 677.

[61] Ibid., 679.

[62] Mullender, "Not a Suicide Pact," 422.

[63] Ibid.

[64] Khawaja, "Not a Suicide Pact," 97–98.

[65] Ibid., 98.

[66] Ibid., 96.

[67] Ibid., 106.

capability of security services in a sustained way to detect terrorist activity is a worse than futile exercise."[68]

3. Civil Liberties

Limiting civil liberties in response to specific threats is seen by some as prudent.[69] As a cost is attached to these limitations, a cost benefit analysis should be used to determine the extent to which civil liberties are constrained.[70] However, the costs are frequently overstated by civil libertarians.[71] Posner argues that civil libertarians are, "Reluctant to acknowledge that national emergencies in general, and the threat of modern terrorism in particular, justify any curtailment of the civil liberties that were accepted on the eve of the emergency."[72] Some argue against the stance that the defense of liberty requires that individuals accept a certain degree of infringement upon their individual liberties.[73] Law Professor Erwin Chemerinsky offers the following opinion, "[I]t is so important for the debate to get past the point where one side is saying, 'We've got to give up civil liberties,' and the other side is saying, 'We cannot give up civil liberties' ... It has to be a much more nuanced discussion of what civil liberties are being compromised, under which circumstances, and for what gain."[74]

4. Security versus Liberty: Case Law

Although an impressive work, the Constitution was written by those who could not fathom the modern world.[75] Khawaja asserts that this document lacks the clarity and specificity necessary to provide guidance on individual liberties.[76] National security has

---

[68] Aaron Brantly, "Banning Encryption to Stop Terrorists: A Worse than Futile Exercise," *CTC Sentinel*, August 2017.

[69] Khawaja, "Not a Suicide Pact," 95.

[70] Ibid., 95–96.

[71] Ibid., 101.

[72] Mullender, "Not a Suicide Pact," 423.

[73] Khawaja, "Not a Suicide Pact," 102.

[74] Arbus, "A Legal U-Turn," 1734.

[75] Khawaja, "Not a Suicide Pact," 95.

[76] Ibid.

been sacrificed in the name of liberty by judges who have been unduly influenced by civil libertarians.[77] However, examples to the contrary exist. In two separate cases, *Bond* (2000) and *Kyllo* (2001), the Supreme Court ruled in favor of individual privacy as it related to indoor and outdoor surveillance using "both low-tech and high-tech surveillance."[78] On the heels of the 9/11 terrorist attacks, airlines provided passenger information to law enforcement.[79] Some passengers sued the airlines for breach of contract, but the court ruled against the plaintiffs.[80]

The adequacy of the Third Party Doctrine has also been called into question.[81] Justice Sotomayor opined, "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[82] Currently, individuals are not safeguarded by the Constitution against information collected from them by online companies.[83] As this information is considered to be willingly provided, companies can legally share it with law enforcement.[84]

Schlabach notes that, "Fast-paced technological change has destabilized the current statutory and constitutional framework for protecting citizens' privacy."[85] He continues, "Simultaneously, it poses a challenge to courts wishing to craft appropriate, narrowly tailored solutions."[86]

This literature review highlights the great divide between privacy experts and government entities, with both sides seemingly unwilling to yield ground. This stalemate has stymied progress and made resolving this issue extremely challenging. The core

---

[77] Khawaja, "Not a Suicide Pact," 96.

[78] Arbus, "A Legal U-Turn," 1766.

[79] Solove, "I've Got Nothing to Hide," 769.

[80] Ibid.

[81] Schlabach, "Privacy in the Cloud," 684–685.

[82] Ibid., 684.

[83] Ibid., 684–685.

[84] Ibid., 691.

[85] Ibid., 697.

[86] Ibid.

concern raised by privacy experts and civil libertarians is that defense of national security is not a valid reason to sacrifice individual privacy, and that government entities cannot be trusted with unlimited power to properly collect, use, manage and dispose of personally identifiable information. Conversely, the government's position is that it is charged with protecting individual citizens and safeguarding national security. Therefore, limiting the tools available to government to complete these tasks makes protecting the country and its citizens, including individual privacy rights exceedingly difficult. This thesis explores these issues in further detail, specifically as they relate to enhanced encryption and the impact it has on law enforcement investigations.

D. RESEARCH DESIGN

Technological advances provide evermore opportunities for law enforcement and bad actors to exploit personal data at the peril of individual privacy rights. Conversely, the United States has endured terrorist attacks, of differing sophistication and damage, in recent years. The December 2015 terrorist attack in San Bernardino highlights the various aspects of this issue from the perspective of law enforcement, privacy experts and businesses. This thesis analyzes this incident in an attempt to determine if it is possible to secure the nation without sacrificing individual privacy rights, and what laws should be revised or newly enacted to fill existing gaps. In addition, the majority of the research that has been conducted to date focuses on the federal government's mass accumulation of data, most notably by the NSA. The review of the San Bernardino case illustrates the difficulties that law enforcement is facing in obtaining information for investigative purposes due to enhanced encryption when armed with proper legal process.

1. Object of Study

This thesis focuses on the deficiencies of existing legislation that are proving to be problematic for law enforcement in accessing electronic communications due to enhanced encryption techniques. Current policy does not address how the private sector is expected to respond to proper legal process regarding these emerging communication platforms or if accommodations can be made to counter enhanced encryption without sacrificing personal privacy and corporate intellectual property.

2. Selection Criteria and Rationale

Research will be conducted on the various types of decryption methods currently available, and the benefits and limitations of each from the perspectives of the various stakeholders, as well as applicable existing legislation. Some of the varying decryption techniques that will be researched include engineering access into a device during the design phase, creating keys that allow access by the designated holder(s), and using system updates to install spyware or a law enforcement friendly operating system. Determining the benefits of each decryption technique depends on the perspective of the stakeholders. Law enforcement may favor the method that guarantees access, such as engineering a point of entry during the design phase. The private sector may prefer a system in which service providers maintain sole control of decryption keys, protecting both their customers and their intellectual property.

3. Instrumentation

The research in this thesis will be comprised of information derived from a review of the literature specifically related to law enforcement's difficulty in accessing communications, encryption/decryption techniques, personal privacy, intellectual property concerns, corporate revenue concerns, and a review of the San Bernardino terrorist investigation.

4. Steps of Analysis

The framework employed for this thesis is the policy analysis method. "This will include clearly defining the problem, researching and testing potential solutions for viability, and putting forth the best recommendation to modify policy and resolve the issue."[87] In addition, to provide context, a review of the investigation regarding the San Bernardino terrorist's iPhone and the Federal Bureau of Investigation's (FBI's) attempt to enlist Apple's assistance in accessing the device will also be employed.

[87] Eugene Bardach and Eric M. Patashnik, *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving* (Thousand Oaks, CA: CQ Press an Imprint of SAGE Publications, Inc., 2016), loc. 192–198 of 3,994, Kindle.

5. Intended Output

The goal of this thesis is to find a solution to an existing problem and make a recommendation on how to address the issue. The intent is that the final recommendation will be used by policy makers to fill legislative gaps and delineate a solution that can be applied to all existing and emerging forms of electronic communications so that law enforcement investigations will not be hampered by enhanced encryption. Chapter II will focus on existing and proposed legislation at the state, federal and international levels. Chapter III will define the "Going Dark" issue and contrast it against what some refer to as the "Golden Age of Surveillance."[88] Enhanced encryption and decryption access techniques will be the subject of Chapter IV. Finally, this thesis will close with a conclusion and recommendations for how policy makers may solve this difficult and controversial issue.

[88] Berkman Center for Internet & Society at Harvard University, *Don't Panic Making Progress on the Going Dark Debate* (Cambridge, MA: Berkman Center for Internet & Society at Harvard University, 2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf; Peter Swire and Joshua Oliver, "The Golden Age of Surveillance," Slate, July 15, 2015, http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

II. CURRENT AND PROPOSED LEGISLATION

This chapter examines existing legislation that provides law enforcement with the authority to intercept communications in the furtherance of investigations. This same legislation gives direction to communication providers and device designers as to their responsibility for providing assistance to government entities when served with proper legal process. Also explored is proposed legislation that may bridge gaps that law enforcement is currently facing due to emerging platforms and enhanced encryption. The concerns of privacy experts and private sector entities, as well as the government's position are also discussed in this chapter.

A. EXISTING LEGISLATION

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 is the legal authority that law enforcement has historically relied upon to conduct communication interceptions.[89] When Title III was initially passed, the types of communications subject to judicially sanctioned interceptions were limited to "wire and aural communications."[90] Law enforcement's interception capabilities were expanded with the passage of the Electronic Communications Privacy Act of 1986 (ECPA).[91] The ECPA increased the government's intercept arsenal by adding electronic communications.[92] However, as technology evolved, law enforcement's ability to successfully conduct communication interceptions was questioned.[93] Congress responded in 1994 by ratifying the "Communications Assistance for Law Enforcement Act," more commonly known as "CALEA."[94] Through CALEA, telecommunication providers and manufacturers were

89 "Title III of The Omnibus Crime Control and Safe Streets Act of 1968," U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, September 9, 2013, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284.

90 Ibid.

91 "Electronic Communications Privacy Act of 1986," Justice Information Sharing, U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, July 30, 2013, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

92 Ibid.

93 Federal Communications Commission, "Communications Assistance for Law Enforcement Act."

94 Ibid.

mandated to engineer or adapt their products to facilitate the continued interception of communications by law enforcement.[95] The advent of "Voice over Internet Protocol (VoIP)" communications provided consumers with the option of using the Internet to place calls rather than relying on traditional analog technology.[96] As a result, CALEA was amended in 2006 to include VoIP communications.[97]

1. CALEA Limitations

Though legal scholars and technology experts disagree over the scope of CALEA, Congress has yet to amend this legislation to remove any ambiguity.[98] Lacking further adjudication, the prevailing wisdom is that CALEA lacks the authority to compel many developing communication platforms to provide law enforcement assistance.[99] Providers like BlackBerry that transmit encrypted email, social networking sites, such as Facebook, companies similar to Skype that provide peer-to-peer messaging, and gaming consoles that provide channels for verbal communication, as well as chat, may not be equipped to comply with Title III Wiretap orders.[100] In addition, the language in CALEA prohibits the government from mandating how companies design their products.[101]

Members of President Obama's administration in 2010 floated the idea of expanding CALEA to fill the gaps created by emerging technologies and enhanced encryption.[102] Potential amendments to CALEA that have been circulated include: (1) requiring companies to decrypt any messages their systems are responsible for

---

95 Federal Communications Commission, "Communications Assistance for Law Enforcement Act."

96 "Voice over Internet Protocol (VoIP)," Federal Communications Commission, November 18, 2010, https://www.fcc.gov/general/voice-over-internet-protocol-voip.

97 Federal Communications Commission, "Communications Assistance for Law Enforcement Act."

98 Kristin Finklea, *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*, CRS Report No. R44187 (Washington, DC: Congressional Research Service, 2016), 6–7, 10, https://fas.org/sgp/crs/misc/R44187.pdf.

99 Federal Bureau of Investigation, "Encryption and Cyber Security."

100 Hibbard, "Wiretapping the Internet," 372–373.

101 Robert Longtin, "Apple, the FBI, and an Act from 1789: The FBI's Impermissible Use of the All Writs Act," *Columbia Business Law Review*, March 28, 2016, https://cblr.columbia.edu/apple-the-fbi-and-an-act-from-1789-the-fbis-impermissible-use-of-the-all-writs-act/.

102 Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet," *New York Times*, September 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=3&hpw&.

encrypting, (2) requiring global companies with U.S. customers to comply with court orders by establishing U.S. offices, (3) requiring peer-to-peer providers to engineer their programs to permit wiretap, and (4) assessing levies for lack of compliance.[103] Most importantly, any amendments to CALEA would be crafted in such a way as to prevent the language from becoming outdated as technology progresses.[104]

The Internet does not currently fall under the purview of CALEA, so although it is possible to wiretap, many providers do not create interception capabilities until they receive proper legal process.[105] Wiretaps of the Internet are different than standard telephone interceptions.[106] Telephone interceptions are typically done at a switch, whereas Internet interception would likely have to be done at endpoints since Internet communications are delivered in packets, which may be broken up along transit.[107] These packets are then delivered and restored at the endpoints through the path with the lowest traffic flow.[108] Designing access points for interceptions creates vulnerabilities.[109] Theoretically, nation-states could exploit these access points and spy on American citizens and corporations.[110]

Critics also argue that the private sector would have to bear the brunt of costs to become compliant and that the proposed changes would hinder technological advancements.[111] Apple has claimed that forcing the company to write code that it does not wish to write and is not in its best interest violates the First Amendment.[112] Code is considered speech, and Apple believes fulfilling this request would be tantamount to

---

[103] Hibbard, "Wiretapping the Internet," 376.

[104] Ibid.

[105] Ibid., 377.

[106] Ibid., 384.

[107] Ibid.

[108] Ibid.

[109] Ibid., 385.

[110] Ibid., 386.

[111] Ibid., 390.

[112] Etzioni, "Apple Good Business?" 7.

"compelled speech."[113] Apple also claimed that being required to write code is a Fifth Amendment violation, equivalent to "forced labor or conscription."[114] During a March 2016 hearing, Georgia Representative Trey Gowdy made the point that when legally compelled, medical professionals are required to remove bullets from unwilling potential defendants for evidentiary purposes, and individuals are forced to submit to blood withdrawals when suspected of driving under the influence.[115] Gowdy continued, "So if you can penetrate the integrity of the human body in certain categories of cases, how in the hell you can't access a phone, I just find baffling."[116]

The government argues that it is not seeking additional powers; it is merely trying to keep pace with criminals who are changing their methods of communication.[117] The government also asserts that engineering interception capabilities would create less vulnerability than modifying the design after the fact.[118] As for the claim that amending CALEA would impede innovation, the telephone companies made the same assertion in regards to cellular telephones when the law was first enacted, but the market became extremely profitable.[119]

2. All Writs Act

In the case of the San Bernardino terrorists, the FBI served Apple with legal process via the All Writs Act (AWA) to gain access to an iPhone used by one of the shooters.[120] This legislation was passed in 1789 and is intended for use when no other legislation is appropriate.[121] The language of the statute reads:

---

[113] Etzioni, "Apple Good Business?"

[114] *The Encryption Tightrope: Balancing Americans' Security and Privacy—Hearing: Committee on the Judiciary, House of Representatives*, 114th Cong. 2 (2016), 152, https://judiciary.house.gov/wp-content/uploads/2016/02/114-78_98899.pdf.

[115] Ibid., 57.

[116] Ibid.

[117] Hibbard, "Wiretapping the Internet," 392.

[118] Ibid., 394.

[119] Ibid.

[120] Longtin, "Apple, the FBI, and an Act from 1789."

[121] Ibid.

> (a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.[122]
>
> (b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.[123]

As the FBI was specifically requesting that Apple load an operating system onto the device so that the government could break the device password, the agency thought use of the AWA was appropriate.[124] Apple's legal team thought otherwise and litigation ensued.[125] The judge in this case asked Apple if complying with this request would result in an excessive burden to the company.[126] Apple replied that unlocking one device would not constitute such a burden, but that costs increase with each additional device the government seeks to access and, "compliance with the court order could substantially tarnish Apple's brand.[127] Before the case could be fully adjudicated, the FBI withdrew its request because a third-party, acting on the agency's behalf, gained access to the device.[128]

Though technology companies cite customer privacy as a major concern, there is public support for compliance. A February 2016 Pew poll revealed that 51% of Americans surveyed thought that Apple should assist the FBI by unlocking the device obtained from the San Bernardino shooter.[129] The poll also showed that 38% were

---

[122] Longtin, "Apple, the FBI, and an Act from 1789."

[123] Ibid.

[124] Hosagrahar Visvesvaraya Jagadish, "Passwords, Privacy and Protection: Can Apple Meet FBI's Demand without Creating a 'Backdoor'?," *Scientific Computing*, February 24, 2016, http://search.proquest.com.libproxy.nps.edu/docview/1777528493/abstract/E615D3E0B2B0447APQ/6; Longtin, "Apple, the FBI, and an Act from 1789."

[125] Felix Wu, "No Easy Answers in the Fight over iPhone Decryption," *Communications of the ACM* 59, no. 9 (September 2016): 20.

[126] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report* (Manhattan, NY: District Attorney, New York County, 2016), 20, http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

[127] Ibid.

[128] Wu, "No Easy Answers," 20.

[129] "More Support for Justice Department than for Apple in Dispute over Unlocking iPhone," Pew Research Center for the People and the Press, February 22, 2016, http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/.

opposed to Apple complying with the request and 11% undecided.[130] In addition, Apple's assertion that its customer's privacy was paramount rings somewhat hollow in light of the German litigation in which the company was embroiled.[131] In 2012, the "Federation of German Consumer Organisations" initiated legislation against Apple for "unfair contractual clauses."[132] Specifically, Apple shared aggregated customer data with its associated businesses, and reserved the right to exploit this data to enhance and market the company's devices and capabilities.[133] In addition, Apple stored personally identifiable information on relatives and others that its customers provided when purchasing gift certificates or accessing other services.[134] The German court ruled that Apple infringed upon the country's privacy laws by allowing for far-reaching use of customer data.[135] Customers did not know how their information was being used and the offended parties also lacked control of the data that was accumulated without their knowledge.[136] Apple's policies in the United States are comparable, and the deployment of enhanced encryption does not prevent the company from collecting customer data for its own use.[137]

B. PROPOSED LEGISLATION

This section covers proposed federal, state and international legislation. Bi-partisan federal legislation has been proposed to address this issue, but to date has not gained the traction necessary for passage.[138] Similarly, legislators in New York,

---

130 Pew Research Center for the People and the Press, "More Support for Justice Department."

131 Anonymous, "Apple's Privacy Headache Intensifies," *Information Management* 47, no. 4 (July–August 2013): 18.

132 Loek Essers, "Apple's Privacy Policy Violates German Data Protection Law, Berlin Court Rules," Computerworld, May 7, 2013, http://www.computerworld.com/article/2497084/data-center/apple-s-privacy-policy-violates-german-data-protection-law--berlin-court-rules.html.

133 Ibid.

134 Ibid.

135 Anonymous, "Apple's Privacy Headache Intensifies."

136 Essers, "Apple's Privacy Policy Violates German."

137 Anonymous, "Apple's Privacy Headache Intensifies"; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 5.

138 "Personal Data Encryption," *Congressional* 95, no. 6 (June 2016).

California and Louisiana have introduced legislation for their respective states, but none have been signed into law.[139] Conversely, several countries around the world have enacted legislation that affords the government the ability to access electronic communications conducted via various platforms.[140] Perhaps these varying laws could be analyzed to determine if they could be employed in whole or in part in federal legislation.

1. Federal Legislation

Senators Richard Burr (NC-R) and Dianne Feinstein (CA-D) have drafted legislation to compel companies to decrypt data when served with proper legal process.[141] The bill, known as the "Compliance with Court Orders Act," requires that companies provide the government with data in a decrypted format if the companies' features were responsible for encrypting the data.[142] Technology companies oppose the act, stating that it will undermine the security of their devices and erode consumer trust.[143] Ron Wyden, a Democratic Senator from Oregon, also opposed the measure, claiming it will make it illegal for Americans to protect their privacy.[144] The Manhattan District Attorney supports this Act, but believes that it falls short in limiting the types of crime eligible for coverage.[145]

The Manhattan District Attorney's office authored a November 2015 report suggesting that the Federal government leverage the Commerce Clause to oblige technology firms and communication providers to make smartphone content available to

---

[139] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 25, 26.

[140] Ibid., 27, 28; Dorle Hellmuth, "Countering Jihadi Terrorists and Radicals the French Way," *Studies in Conflict and Terrorism*, August 24, 2015, http://www.tandfonline.com/loi/uter20; Carla Bleiker, "New Surveillance Law: German Police Allowed to Hack Smartphones," Deutsche Welle, June 22, 2017, http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085.

[141] *Congressional*, "Personal Data Encryption."

[142] Ibid.

[143] Ibid.

[144] Ibid.

[145] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 31.

law enforcement.[146] The assertion is that through this Clause, Congress has the authority to regulate goods that impact commerce, and a statute could be drafted to ensure smartphone access.[147] The Manhattan DA wrote a follow-up report one year later suggesting legislation be enacted to compel device designers to preserve their ability to obtain data from phones when served with proper legal process.[148] The intent of this proposed legislation is to reset the situation to that which was present prior to Apple releasing iOS 8.[149] The report's authors compare this proposed legislation to similar product safety laws, such as those requiring, "buildings to be constructed with exits and egresses that satisfy specific requirements, and roads to have maximum speed limits."[150]

2. State Legislation

Legislation has been introduced at the state level by New York, California and Louisiana.[151] In 2015, New York initiated legislation known as "Assembly Bill A.8093A."[152] This legislation stipulates that manufacturers retain the ability to decrypt or unlock all smartphones sold or leased in the state. Smartphone vendors that fail to comply would be subject to fines of $2,500 per device sold or leased. The New York bill has Democratic support, but it is unknown if it will be passed.[153] California introduced Assembly Bill 1681 that mimics New York's bill except that the $2,500 fine would be imposed against device or operating systems designers, not sellers.[154] The legislation also

---

[146] "Commerce Clause," Legal Information Institute, Cornell University Law School, July 3, 2008, https://www.law.cornell.edu/wex/commerce_clause; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety* (Manhattan, NY: District Attorney, New York County, 2015), 13, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

[147] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, 13.

[148] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 15.

[149] Ibid.

[150] Ibid.

[151] Ibid., 24–25.

[152] Ibid., 24.

[153] Ibid., 25.

[154] Ibid.

specifies that companies cannot pass these fines onto their customers.[155] This bill lost traction in April 2016 and it is unknown if it will be retooled in hopes of passage.[156] Louisiana introduced House Bill 1040, also known as the Louisiana Brittney Mills Act in April 2016.[157] The impetus for this bill was the murder of a woman, Brittney Mills, who was eight months pregnant.[158] Mills' baby, who was delivered the day that she was killed, died one week later.[159] This bill was introduced because the victim's phone was found at the crime scene and law enforcement believes the device may contain clues that could lead them to the perpetrator.[160] Unfortunately, the phone is locked and law enforcement has not been able to gain access to the device or its contents, resulting in a stalled investigation.[161] The Louisiana legislation is identical to New York's proposed bill, with one exception.[162] If the user of the device is a homicide victim, then the Attorney General is compelled to fine the seller or lessor, rather than having the option of seeking financial penalty.[163] However, this bill has not yet passed.[164] The most recent vote ended in a tie, with the opposition favoring federal legislation as a remedy.[165] This bill is expected to be presented again at a later date.[166]

Those opposed to using state legislation to address the encryption issue offer several reasons. Some legislators favor federal legislation over that of the state because of issues caused by frequent device portability.[167] A user may change providers at will and

---

[155] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 25.

[156] Ibid.

[157] Ibid.

[158] Ibid., 25–26.

[159] Ibid., 26.

[160] Ibid.

[161] Ibid.

[162] Ibid.

[163] Ibid.

[164] Ibid.

[165] Ibid.

[166] Ibid.

[167] Ibid., 29.

maintain his/her phone number. This means that for the duration of the period that the device is held by a user, it may be serviced by multiple providers in several states. Another reason some legislators prefer federal legislation is that New York and Louisiana's proposed legislation seeks to penalize phone vendors in their respective states.[168] However, if this legislation is passed, then vendors will likely relocate to neighboring states to continue their business.[169] Regarding California's proposed legislation, the recommended fines would only apply to devices that law enforcement attempted to access but could not.[170] Therefore, the amounts would be too small in comparison to corporate revenues for them to act as effective deterrents.[171]

3. International Legislation

Citizens in Singapore and the United Kingdom must now provide their passcodes to law enforcement when legally compelled, or face criminal penalties.[172] The United Kingdom can impose five-year sentences for non-compliance, while those in Singapore may face three years in prison, and/or a $10,000 fine for individuals who refuse to provide their passcodes for device decryption.[173] Similar laws would not likely be passed in the United States, as they would infringe upon Fifth Amendment rights.[174] The United Kingdom has also introduced additional legislation that has been approved by the House of Commons and is being reviewed by the House of Lords.[175] This new legislation compels communication providers to disable any encryption that the provider has engineered into its devices.[176] Companies are afforded the option of appealing to the

---

[168] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 30.

[169] Ibid.

[170] Ibid

[171] Ibid.

[172] Ibid., 27.

[173] Ibid.

[174] Ibid.

[175] Ibid., 28.

[176] Ibid., 27–28.

Secretary of State if they deem the process to be a financial burden or impractical request.[177] Foreign companies are not bound by this pending legislation.[178]

Police in France were granted the authority in 2011 to install spyware on target computers, allowing for real time, covert examinations.[179] In addition, French lawmakers are considering legislation that would imprison and fine technology executives for spurning law enforcement's requests to access devices in terrorism cases.[180]

Germany passed legislation in June 2017, known as the Source Telecommunications and Online Surveillance Law.[181] This legislation provides German law enforcement with the authority to install spyware onto a target device and view content in the same manner as the user.[182]

The Netherlands considered legislation that would compel communication providers and device designers to cooperate with law enforcement in accessing encrypted data.[183] However, in January 2016, the government declared that it would not seek to enact this law.[184]

European Union members France and Germany brought the encryption issue to the forefront in August 2016, when they suggested that the coalition implement requirements compelling communication providers to assist law enforcement with access to encrypted data.[185] The collaborative effort focused on accessing communications in

---

[177] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 28.

[178] Ibid.

[179] Hellmuth, "Countering Jihadi Terrorists and Radicals the French Way."

[180] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 28.

[181] Jefferson Chase, "Things to Know about Germany's Recent Surveillance Laws," Deutsche Welle, June 26, 2017, http://www.dw.com/en/things-to-know-about-germanys-recent-surveillance-laws/a-39421060.

[182] Bleiker, "New Surveillance Law: German Police Allowed to Hack Smartphones."

[183] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*.

[184] Ibid.

[185] Ibid.

terrorist investigations while safeguarding individual privacy.[186] The status of this proposal is unknown.

As of July 2017, China has mandated that Apple remove applications from its App Store that allow Chinese citizens to bypass the country's firewall.[187] Chinese officials claim that these networks are illegal in their country, while those opposed claim that by complying Apple is effectively facilitating censorship.[188] Apple is complying with this mandate.[189] China is second only to the United States in Apple's market share.[190]

C. STAKEHOLDER STANDPOINTS

This section examines the varied positions of the main stakeholders. Privacy experts claim that softening encryption in any way would pose a danger to all users.[191] Whereas, technology companies fear that intellectual property would be at risk if back doors were introduced into their products.[192] Conversely, law enforcement maintains the position that design designers and communication providers could provide required assistance without unduly compromising individual privacy or corporate intellectual property.[193] Following is a more detailed review of the chasm between the various stakeholders.

---

[186] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*.

[187] Rishi Iyengar, "Apple Is Removing VPN Apps that Allow Users to Skirt China's Great Firewall," CNN Money, July 29, 2017, http://money.cnn.com/2017/07/29/technology/china-apple-app-store-vpn-express/index.html.

[188] Ibid.

[189] Ibid.

[190] Ibid.

[191] Abelson et al., "Keys under Doormats," 2.

[192] Michael G. Crowley and Michael N. Johnstone, "Protecting Corporate Intellectual Property: Legal and Technical Approaches," *Business Horizons* 59, no. 6 (November–December 2016): 627.

[193] H.R., *Encryption Tightrope,* 190.

1. Privacy Concerns

Many privacy experts assert that providing law enforcement with the access it requires would undermine security for all users.[194] Once it becomes known that devices have particular vulnerabilities, then bad actors will work to identify and exploit the weaknesses.[195] Corporations are also concerned that these vulnerabilities may be used to gain access to their code and reverse engineer their products.[196] However, many of the highly-publicized cyber-attacks that have recently occurred were the result of malware, phishing or outdated security software.[197] Enhanced encryption does not guard against these vulnerabilities; therefore, the attacks on Target (2014), the Office of Personnel Management (2015) and the Democratic National Committee (2016) would have still occurred even if enhanced encryption were in place.[198] Instead, enhanced encryption impedes law enforcement's capability to thoroughly investigate these and similar crimes.[199] Many technology companies tout enhanced encryption as a major selling point and claim that their international sales would suffer if forced to modify their encryption.[200] The State Department and the Commerce Department have warned that foreign governments hostile to their own citizenry may exploit known vulnerabilities to persecute dissidents.[201]

2. Government Perspective

Apple and Google claim that their most recently released operating systems were engineered with enhanced encryption to protect their customers and corporate intellectual

---

194 Abselson et al., "Keys under Doormats," 2.

195 Ibid.

196 Crowley and Johnstone, "Protecting Corporate Intellectual Property," 627.

197 District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 4–5.

198 Ibid.

199 Ibid.

200 Timberg, "Newest Androids"; Bankston, "It's Time to End the 'Debate.'"

201 Hibbard, "Wiretapping the Internet," 391.

property.[202] However, the Manhattan District Attorney's report asserts that no known vulnerabilities were reported that would have accounted for both companies engineering such significant changes.[203] Further, the report states that a bad actor would need physical custody of a specific device in order to access the content.[204] Therefore, even if one were to illegally gain access to Apple's decryption methods, access would be denied without the device.[205]

What is puzzling is why both companies comply with legal process when it comes to customer data stored on the cloud.[206] Why have Apple and Google made the engineering decision to make cloud-stored data accessible, and not data stored on individual devices?[207] Apple states in its legal process guidelines that the company is able to access some customer data stored via iCloud because it maintains custody of encryption keys.[208] Apple's General Counsel testified that data stored on the cloud is indeed encrypted, but not in the same way as its phones.[209] Examples of some of the data available from iCloud include text, email and voicemail messages.[210] However, following the Snowden leaks, Apple made the conscious decision, which it also used as a marketing tool, to engineer devices using iOS 8 or later with end-to-end encryption removing the company from the access equation.[211] If Apple is sincere in its argument

---

[202] Crowley and Johnstone, "Protecting Corporate Intellectual Property," 626; Timberg, "Newest Androids."

[203] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 14.

[204] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*.

[205] Ibid.

[206] Ibid., 15.

[207] Ibid.

[208] Apple, *Legal Process Guidelines, Government and Law Enforcement within the United States* (Cupertino, CA: Apple, 2017), https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

[209] H.R., *Encryption Tightrope*, 155.

[210] Apple, *Legal Process Guidelines*.

[211] Ibid.; Timberg, "Newest Androids."

that it is fighting the government to preserve customer privacy, why does it maintain iCloud encryption keys?[212]

It should also be noted that the deployment of enhanced encryption would not have shielded the public from the massive data collection carried out by the NSA, which seems to be the impetus for Apple's decision to lock out law enforcement.[213] Apple itself was reported to be one of nine companies that previously participated in the NSA's PRISM program.[214] PRISM reportedly allowed the NSA direct server access to communications from the participating entities.[215] Apple and Google have denied granting the NSA such access.[216]

The Manhattan DA attempted to engage both Apple and Google to determine the companies' respective perceived threats that led the corporations to alter their designs and deploy enhanced encryption.[217] The DA sent letters to both companies in hopes of obtaining answers to the following questions, with the first inquiry pertaining only to Apple:[218]

> If Apple kept a "key" so that it was able to unlock iPhones, would the iPhones be more vulnerable to hackers than if Apple had no such "key"? Is there any "key" or similar device that Apple might keep without sacrificing the security of iPhones from hackers? Is there a way to measure

---

[212] Jose Pagliery, "Apple Promises Privacy—But Not On iCloud," CNN Money, February 22, 2016, http://money.cnn.com/2016/02/22/technology/apple-privacy-icloud/index.html.

[213] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 5.

[214] Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps into User Data of Apple, Google and Others," *Guardian*, June 7, 2013, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1; Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post*, June 7, 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.b263741a8ae2.

[215] Ibid.

[216] Ibid.

[217] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 13–14.

[218] Ibid.

> or quantify the vulnerability to hackers of iPhones (a) if Apple kept a key, as compared to (b) if it did not keep a key?[219]
>
> In iOS 7 and prior operating systems, and in Android systems prior to Lollipop 5.0, if an attacker learned Apple's or Google's decryption process, could [the attacker] use it to remotely attack devices or would he need possession of the device?[220]
>
> What technical problem does the full-disk encryption of iOS 8 and Lollipop 5.0 solve? Quantify the problem to the extent possible**.** For example, if the largest security threat posed by prior systems was a hacker hacking Apple's or Google's systems to gain access to the decryption process, what are the chances of this? Has it happened before? If the largest security threat posed by prior systems was an insider improperly sharing Apple's or Google's decryption process, has this happened before? What security protocols are in place to make sure this doesn't happen? What are the chances of them being breached?[221]

Neither Apple nor Google responded to the Manhattan DA's inquiry.[222] However, below is an exchange between Bob Goodlatte, Chairman of the Committee on the Judiciary House of Representatives and Apple's Senior Vice President and General Counsel Bruce Sewell, which occurred in writing subsequent to the March 2016 testimony.

> **Goodlatte**: How did Apple decrypt iPhones operating on the iOS 7 or an earlier operating system? Was this done remotely or in-house?
>
> **Sewell:** In the past, using an in-house process, Apple was able to extract data that was not protected by passcode-protected encryption. This applies to iPhones running iOS 7 and earlier operating systems.
>
> **Goodlatte**: Was the technology you possessed to decrypt these phones ever compromised?

---

[219] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 13.

[220] Ibid., 13–14.

[221] Ibid., 14.

[222] Ibid., 13–14.

> **Sewell:** The process Apple used to extract data from locked iPhones running iOS 7 or earlier operating systems was not, to our knowledge, compromised.[223]

Apple's response counters the private sector argument that enhanced encryption was added to safeguard customer privacy and intellectual property. Providers have previously claimed that maintaining decryption keys creates significant insider and hacking threats.[224] However, Apple's General Counsel acknowledged on the record that Apple's prior operating systems that lacked enhanced encryption were never compromised.[225]

D. REASONS FOR IMPASSE

Over time, the relationships that law enforcement previously enjoyed with the corporate world appear to have deteriorated. For instance, CALEA was enacted to mandate that telecommunication providers engineer their devices and systems in such a way as to provide law enforcement with assistance in accessing communications.[226] As directed, these providers made the required modifications and complied with this law. Now, Apple argues that being forced to assist law enforcement violates the corporation's First and Fifth Amendment rights.[227] In addition, Apple claims that its decision to enhance device encryption was based on the company's desire to protect individual privacy.[228] However, the corporation's own practices led German courts to rule that Apple infringed upon that country's privacy laws.[229] Admittedly, legislation has not kept pace with the myriad forms of emerging communication platforms and enhanced encryption techniques. Various pieces of legislation have been proposed at the state and

---

[223] H.R., *Encryption Tightrope*, 190.

[224] Kristin Finklea, Richard M. Thompson II, and Chris Jaikaran, *Court-Ordered Access to Smart Phones: In Brief*, CRS Report No. R44396 (Washington, DC: Congressional Research Service, 2016), 6, https://fas.org/sgp/crs/misc/R44396.pdf.

[225] H.R., *Encryption Tightrope*, 190.

[226] Federal Communications Commission, "Communications Assistance for Law Enforcement Act."

[227] Etzioni, "Apple Good Business?", 8; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 152.

[228] Crowley and Johnstone, "Protecting Corporate Intellectual Property," 626.

[229] Essers, "Apple's Privacy Policy Violates German."

federal levels, and some more stringent laws have been passed in other countries. Through judicial and legislative debates, privacy experts stand firm in their belief that providing government with the access it requires would necessitate introducing vulnerabilities that could be exploited by bad actors, thereby endangering individual privacy, dissident safety, intellectual property and corporate profits.[230] The government on the other hand questions why Apple and Google have gone to such lengths to enhance their encryption when Apple confirmed that the process it previously used to assist law enforcement had never been compromised.[231] Further, law enforcement stresses that it is not seeking additional powers.[232] Agencies merely want to maintain the ability to access communications so that they can successfully fulfill their respective missions unhindered.[233] Clearly, the stakeholders are separated by a deep chasm due to their disparate views and motivations. These differences may present the largest hurdle in solving this problem.

[230] Abelson et al., "Keys under Doormats," 2; Crowley and Johnstone, "Protecting Corporate Intellectual Property," 627; Hibbard, "Wiretapping the Internet," 391.

[231] H.R., *Encryption Tightrope*, 190.

[232] Hibbard, "Wiretapping the Internet," 392.

[233] Ibid.

III. "GOING DARK" VERSUS THE "GOLDEN AGE OF SURVEILLANCE"

This chapter assesses the claim espoused by some privacy experts that new technology may actually provide law enforcement with innovative intercept capabilities that may compensate for the access they lose due to enhanced encryption. The reporting of wiretap statistics, and their availability and subsequent impact are also discussed. Included in these statistics are some of the types of crime where electronic interceptions are employed.

A. THE "GOING DARK" DEBATE

Valerie Caproni, the former General Counsel for the FBI, defined the "Going Dark" phenomenon as follows: "The widening gap between law enforcement's legal privilege to intercept electronic communications and its practical ability to actually intercept those communications."[234] This gap has widened further still as Facebook announced that it will make it easier for its 900 million users to encrypt their communications.[235] As it now stands, targets of investigation can communicate surreptitiously on various platforms free from detection.[236] James Comey, the former Director of the FBI, has warned that law enforcement is facing the issue of "Going Dark" in regards to accessing communications that were previously available.[237] In March 2016, Comey gave testimony before the Committee on the Judiciary House of Representatives in which he stated that, "technology has allowed us to create zones of complete privacy."[238] Comey further stated that these "zones prohibit any government

[234] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 5–6.

[235] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 12.

[236] Ibid.

[237] "Counterterrorism, Counterintelligence, and the Challenges of Going Dark," Federal Bureau of Investigation, July 8, 2015, https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark.

[238] H.R., *Encryption Tightrope*, 52.

action under the Fourth Amendment or under our search authority."[239] Representative Henry Johnson Jr. from Georgia replied, "Well, it's actually a zone of impunity, would it not be, a zone where bad things can happen and the security of Americans can be placed at risk?"[240] Representative Trey Gowdy from South Carolina added, "the right to counsel, the right to free speech, the right to a jury trial just isn't of much use if you are dead, so I reconcile those competing principles in favor of public safety."[241] Gowdy commented further, "National security, there's nothing that the government has a more compelling interest in than that, and we're going to create evidence-free zones?"[242] Representative Gowdy closed his remarks by commenting on Apple's stance in regard to the San Bernardino case:

> So Apple, on the one hand, wants us to kind of weigh and balance privacy, except they have done it for us. They have said at least as it relates to this phone, we've already done that weighing and balancing, and there is no governmental interest compelling enough for us to allow you to try to guess the password of a dead person's phone that is owned by a city government. There's no balancing to be done. They have already done it for us.[243]

Cyrus Vance, Jr., the District Attorney for New York County, testified in this same hearing that criminals use electronic devices to plot and carry out their illicit activity, and they are very much aware that enhanced encryption provides a safe communications haven.[244] DA Vance added the following anecdote to his testimony. "In one lawfully recorded phone conversation from Rikers Island in New York, an inmate, talking about the iOS 8 default device encryption, called it, and I'm quoting, 'a gift from God.'"[245] DA Vance supplemented his testimony with the following statement:

---

[239] H.R., *Encryption Tightrope*, 52.

[240] Ibid.

[241] Ibid., 56.

[242] Ibid.

[243] Ibid.

[244] Ibid., 131.

[245] Ibid.

> So centuries of jurisprudence that have been talked about today have held that no item, not a home, a file cabinet, a safe, or even a smartphone, is beyond the reach of a court-ordered search warrant. But the warrant-proof encryption today gives two very large companies, we believe, functional control over the path to justice for victims of crime, including who could be prosecuted and, importantly, who may be exonerated.[246]

DA Vance submitted the following as part of his written statement to the committee members:

> In the absence of uniform policy, our nation will effectively delegate the crafting of national security and law enforcement policy to board rooms in Silicon Valley. That is, important responsibilities of our government will be carried out by Apple, Google and other technology companies, who will advance the best interests of their shareholders, not necessarily the best interests of our nation.[247]
>
> Technology companies should not be able to dictate who can access key evidence in criminal investigations. No device or company, no matter how popular, should be able to exempt itself from court obligations unilaterally.[248]

DA Vance submitted the following to the committee in a written exchange following his March 2016 testimony:[249]

> **Chairman Goodlatte:** "In your law enforcement career, how would you rank this issue of encryption in terms of complicating investigations?"[250]
>
> **Vance:** "Apple's introduction of a product that is beyond the reach of a search warrant into the stream of commerce is—and marketing the product as warrant-proof – is entirely unprecedented. One of the largest companies in the world intentionally and explicitly frustrating its own ability to comply with court orders is entirely unprecedented."[251]

Police in Toronto, Canada, have reported reading chat messages between pedophiles stating that those operating in the United States are at an advantage because

---

[246] H.R., *Encryption Tightrope*, 132.

[247] Ibid., 134.

[248] Ibid., 145.

[249] Ibid., 213.

[250] Ibid.

[251] Ibid.

they cannot be compelled by law enforcement to reveal their passcodes.[252] The author(s) of the chat messages maintained that refusing to reveal passcodes will not result in incarceration, instead, law enforcement will be forced to close the case due to lack of evidence.[253]

B. "THE GOLDEN AGE OF SURVEILLANCE"

In contrast to the "Going Dark" issue, some privacy experts have asserted that law enforcement is enjoying the "Golden Age of Surveillance" due to the accessibility of metadata and the introduction of the Internet of Things (IoT).[254] Both sources have the potential to be exploited in a myriad of ways to identify subjects and speed case progression.[255] Privacy experts contend that the public's willingness to adopt technological innovations provides the government with an advantage.[256] The most recent example is the popular in-home electronic assistant. Amazon reportedly sold millions of the company's versions, known as Alexa and Echo during the 2017 holiday season.[257] These devices perform a variety of tasks based on voice commands, such as controlling the thermostat and lights in one's home, placing telephone calls, and arranging trips.[258] In-home electronic assistants and other IoT devices offer the potential to intercept conversations and collect video and other useful data from a subject's home.[259] In addition, law enforcement has successfully served proper legal process on OnStar and similar companies to obtain audio and geo-location information from subject

---

[252] Mark Greenblatt and Robert Cribb, "Encrypted Evidence Is Increasingly Hampering Criminal Investigations, Police Say," November 6, 2015, http://www.wcpo.com/news/national/encrypted-evidence-is-increasingly-hampering-criminal-investigations-police-say?page=2.

[253] Ibid.

[254] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 1, 3.

[255] Swire and Oliver, "The Golden Age."

[256] Ibid.

[257] Lauren Thomas, "Amazon's Echo Dot Has Record Holiday Weekend, Millions of Devices Sold," CNBC, November 28, 2017, https://www.cnbc.com/2017/11/28/amazons-echo-dot-has-record-holiday-weekend-millions-of-devices-sold.html.

[258] Carley Knobloch, "11 Reasons We Love Amazon Alexa (and Why You Should Buy One Right Now)," Today, December 27, 2017, https://www.today.com/home/best-amazon-alexa-skills-echo-dot-show-t115489.

[259] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 13–14.

vehicles.[260] Another example of the public's widespread adoption of technology is the prodigious use of text messages to communicate during the last 25 years.[261] CNN reported in 2012 that U.S. citizens send 2.2 trillion text messages annually.[262] Professor and privacy expert Peter Swire claims that providers can provide law enforcement with the content of the majority of text messages.[263] Swire contends that law enforcement's access to metadata for those text messages that are encrypted should not be discounted.[264] Prior to the widespread adoption of electronic communications, many meetings between investigative targets could remain clandestine.[265] Now, privacy experts maintain, the accessibility of metadata provides law enforcement with the ability to identify an individual's pattern of life and close associates.[266] These associates could then be exploited to further an investigation.[267] However, as the Snowden leaks became public, more and more providers added or enhanced their encryption. In addition, metadata is only useful to a point. In the case of a kidnapping or terrorist act or plot, access to content is vital. Dates, times, durations of calls, as well as the other party's phone number will not disclose where a victim may be held or when and where an attack is planned. Privacy experts have conceded that there are certain devices and communications that law enforcement is unable to access due to enhanced encryption, but maintain that the extensive digital footprints that are created by the public present a trove of information.[268]

---

[260] Thomas Fox-Brewster, "SiriusXM Satellite Radio Tech Turned into Surveillance Device," *Forbes*, January 15, 2017, https://www.documentcloud.org/documents/3295672-SiriusXM-Satellite-Radio-Tech-Turned-Into.html.

[261] Heather Kelly, "OMG, The Text Message Turns 20. But Has SMS Peaked?" CNN, December 12, 2012, http://www.cnn.com/2012/12/03/tech/mobile/sms-text-message-20/index.html.

[262] Ibid.

[263] Swire and Oliver, "The Golden Age."

[264] Ibid.

[265] Ibid.

[266] Ibid.

[267] Ibid.

[268] Ibid.

C. FACTORS CONTRIBUTING TO STAKEHOLDERS' VARYING VIEWS

This section explores the various issues that may be contributing to the divergent stakeholder positions. Legislators and privacy experts may be unaware of the depth of the problem due to an underreporting of statistics.[269] In addition, certain communication platforms have become impossible to intercept, leading law enforcement to eschew seeking legal process altogether and leaving these instances unreported.[270] Law enforcement may also be concerned with alienating the judiciary if they pursue intercepts where success in obtaining the required information is questionable.[271] Furthermore, to remain effective, law enforcement is intensively protective of its capabilities and its limitations. Finally, until somewhat recently, there was no mechanism in place to capture statistics for electronic devices seized by state and local law enforcement agencies, further cloaking the extent of the problem.[272] These factors are further explored below.

1. Incomplete Wiretap Statistics

Privacy experts point to the dearth of publically available information to strengthen their argument that law enforcement overstates the threat encryption poses to investigations.[273] Annually, state and federal prosecutors are required to report to the court statistics on Title III wiretap investigations, which the court then reports to Congress.[274] (See the Appendix for an example of the form used by prosecutors to report wiretap statistics to the court.) Included in these statistics is the number of instances that law enforcement has encountered encryption that it could not surmount.[275] These reported statistics are relatively low in comparison to the number of intercepts conducted.[276] However, the statistics reported for 2016 reflect a sharp spike in the

---

[269] United States Courts, "Wiretap Reports."

[270] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 3–4.

[271] Potapchuk, "A Second Bite at the Apple," 1414.

[272] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 10.

[273] Swire and Oliver, "The Golden Age, 1–2; Abselson et al., "Keys under Doormats," 3.

[274] United States Courts, "Wiretap Reports."

[275] Ibid.

[276] Ibid.

number of instances insurmountable encryption was encountered. Additionally, it should be noted that these figures are impacted by reports not received in time to include in the annual statistics and by prosecutors' decisions to delay reporting in order to protect ongoing investigations.[277] The reasoning behind prosecutorial decisions to delay reporting seems to be without merit as no target-specific information is reported.[278] Remarkably, roughly one-third of wiretap statistics are missing from the annual reporting, according to the Administrative Office of the U.S. Courts.[279] The reason for non-compliance with this mandate remains unclear, but if the statistics from 2016 are any indication, the instances of insurmountable may continue to rise. Table 1 breaks down the number of wiretap intercepts, the number of instances that insurmountable encryption was encountered, and the number of intercept statistics not reported during the period 2012–2016. This data encompasses nationwide reporting from state and federal prosecutors.

Table 1. Title III Intercept Statistics[280]

Year	**2012**	**2013**	**2014**	**2015**	**2016**
Total Intercepts	3,395	3,576	3,554	4,148	3,168
Insurmountable Encryption Encountered	4	9	4	11	101
Intercept Statistics Not Reported	846	1,198	1,081	1,369	903
Note: 2012 is the first year insurmountable encryption was reported to the court.					

2. Reluctance to Pursue Electronic Interceptions

This reporting also excludes how often law enforcement declines to pursue an intercept once it is determined that a particular encryption method or application is in use. For instance, it is becoming more widely known that the application WhatsApp uses

[277] United States Courts, "Wiretap Reports."

[278] Administrative Office of the United States Courts, *WT-2A Federal Form* (Washington, DC: Administrative Office of the United States Courts, 2015), http://www.uscourts.gov/sites/default/files/form_wt-2a_0.pdf.

[279] United States Courts, "Wiretap Reports."

[280] Source: Ibid.

encryption methods that law enforcement cannot penetrate.[281] WhatsApp has deployed end-to-end encryption, making it impossible for the company to provide law enforcement with message content.[282] As the process for obtaining judicial authority to conduct an intercept is arduous and time-consuming, not to mention costly if approved, law enforcement is not likely to petition for a WhatsApp or similar intercept. Therefore, the many times that law enforcement encounters these issues and refrains from petitioning for an intercept will not be captured in the statistics reported to the court.

3. Fear Judiciary May Decline Future Requests for Electronic Intercepts

In addition, if law enforcement were to push forward affidavits to the court for all types of devices and applications, regardless of their past interception success rate, the judiciary may be less inclined to approve future requests.[283] As part of the affidavit process, law enforcement is required to prove "exhaustion," which means that all other reasonable methods have been unsuccessful or pose too much of a risk to pursue, leaving the Title III intercept as the only remaining option.[284] However, in the affidavit law enforcement is required to define what it expects to derive from the interception, and if the agency knows that a device or application is impenetrable, then this would have to be disclosed. Neither law enforcement nor the court can afford to waste time on such a laborious process.

4. Law Enforcement's Reluctance to Report Vulnerabilities

The issue is exacerbated by law enforcement's long-time habit of guarding investigative techniques. This protection extends to roadblocks encountered. If criminals and terrorists are aware that a certain device or platform provides impenetrable

---

[281] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 3–4.

[282] Thomas Fox-Brewster, "Forget about Backdoors, This Is the Data WhatsApp Actually Hands to Cops," *Forbes*, January 22, 2017, http://www.forbes.com/sites/thomasbrewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/.

[283] Potapchuk, "A Second Bite at the Apple," 1414.

[284] Wesley Cheng, *A Practitioner's Guide to Wiretaps in Public Corruption Investigations* (New York City: Center for the Advancement of Public Integrity, Columbia Law School, 2016), http://www.law.columbia.edu/sites/default/files/microsites/public-integrity/files/a_pracititioners_guide_to_wiretaps_in_public_corruption_investigations_7.25.2016_0.pdf.

anonymity, they will likely embrace its use. Once a case progresses to the trial phase, many investigative techniques are disclosed. If this disclosure is widely publicized, then criminal entities learn and adapt, placing law enforcement at a disadvantage regarding future investigations. This may explain law enforcement's reluctance to share its successes and failures publicly, except as required by the courts. Hence, the private sector, which is in the best position to assist the government, sees only a fragment of the problem due to the protective practices of law enforcement.

5. Devices in Evidence: Incomplete Reporting of Encryption Issues

A 2016 report prepared by the Manhattan District Attorney's Office highlights the extent of the problem. The Manhattan DA reported that since Apple engineered the iOS 8 with enhanced encryption, the forensics lab under its jurisdiction has been unable to access the contents of 423 devices in its possession.[285] Further, DA Cyrus Vance, Jr., stated that in some cases, investigations have completely stalled due to insufficient information.[286] This number is expected to climb significantly as approximately 96% of all smartphones are Apple or Google devices, and overtime older devices will be replaced with newer models with default encryption.[287] What some may fail to consider is that information extracted from devices is not only used to indict targets, but it may also be used to exonerate the innocent.[288] As these are devices in the possession of law enforcement, they would not have been included in the wiretap statistics reported to the court, since extracting data from seized devices is a different process than conducting electronic intercepts. Nevertheless, the information reported by the Manhattan District Attorney shows how widespread the problem is and that it impacts more than federal law enforcement agencies.

---

[285] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 8.

[286] Rachel Martin, "It's Not Just the iPhone Law Enforcement Wants to Unlock," NPR, February 21, 2016, http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock.

[287] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 9.

[288] Martin, "It's Not Just the iPhone."

For instance, a few state and local law enforcement agencies have reported similar investigative roadblocks, as shown in Table 2.

Table 2. Reported Encryption Issues–State/Local Agencies[289]

Agency	Devices	Crime Category
Harris County DA—TX	8–10 per week	Many Homicides
Suffolk County DA—MA	151	Sex Crimes, Homicides, Larcenies
Los Angeles, CA (Agency not specified)	300	Not Listed
WI Department of Justice	68	Not Listed

The Manhattan District Attorney's office has partnered with state and local law enforcement agencies and the National Domestic Communications Assistance Center to develop a system to better collect and track incidents in which law enforcement encounters insurmountable encryption.[290] A website has been created and as of November 2016, law enforcement agencies from twenty-three states have contributed statistical data.[291] The goal is to gain a more complete picture of how widespread the issue is so that appropriate steps can be taken to rectify the problem.[292]

D. PREVALENCE OF NARCOTICS CASES DIMINISHING ENCRYPTION ISSUE?

The previously cited Pew poll revealed that 51% of Americans thought that law enforcement should be able to access the San Bernardino terrorist's phone.[293] As a result, law enforcement may find that it is possible to garner public support to combat terrorism and solve violent crime. However, the types of crime that Title III interceptions are most typically associated with may pose an issue. Although electronic interceptions are

[289] Source: District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 9–10.

[290] Ibid., 10.

[291] Ibid.

[292] Ibid.

[293] Pew Research Center for the People and the Press, "More Support for Justice Department than for Apple in Dispute over Unlocking iPhone."

certainly employed for terrorist cases and other life-or-death investigations, such as kidnappings, the vast majority are related to narcotics cases.[294] Indeed, Apple accused the FBI of cherry-picking the San Bernardino terrorist case in the hopes of swaying the public, judiciary and lawmakers alike.[295] As more states legalize marijuana for medical, as well as personal use, public support for intercepts related to narcotic investigations could wane. The acceptance of drug use may cause a shift in the court of public opinion, resulting in lawmakers reallocating taxpayer dollars and law enforcement assets to areas other than narcotics.

However, even if legislators and members of the public become more tolerant of drug use and less concerned with prosecuting narcotic-related crimes, there is another issue worthy of consideration. There have been documented cases of narcotics proceeds being used to facilitate terrorist financing.[296] Hezbollah, in order to sponsor terrorist activities, is reported to be in collusion with South American drug cartels to smuggle large quantities of cocaine.[297] The United Nations Office on Drugs and Crime reported that when Madrid suffered a terrorist attack, narcotics were used as currency.[298] Therefore, it is not out of the realm of possibility that successful narcotics investigations could potentially disrupt terrorism.

For purposes of Figure 1, only violent crimes and narcotics were included. It should be noted that in the wiretap statistics reported to the court, terrorism is not listed as a criminal category.[299] Violent crimes are segmented and a catch-all category labeled "Other" is also used.[300]

---

294 United States Courts, "Wiretap Reports."

295 Etzioni, "Apple Good Business?"

296 Guy Taylor, "Hezbollah Moving 'Tons of Cocaine' in Latin America, Europe to Finance Terror Operations," *Washington Times*, June 8, 2016, http://www.washingtontimes.com/news/2016/jun/8/hezbollah-moving-tons-of-cocaine-in-latin-america-/.

297 Ibid.

298 "Drug Trafficking and the Financing of Terrorism," United Nations Office on Drugs and Crime, accessed June 16, 2017, http://www.unodc.org/unodc/en/frontpage/drug-trafficking-and-the-financing-of-terrorism.html.

299 United States Courts, "Wiretap Reports."

300 Ibid.

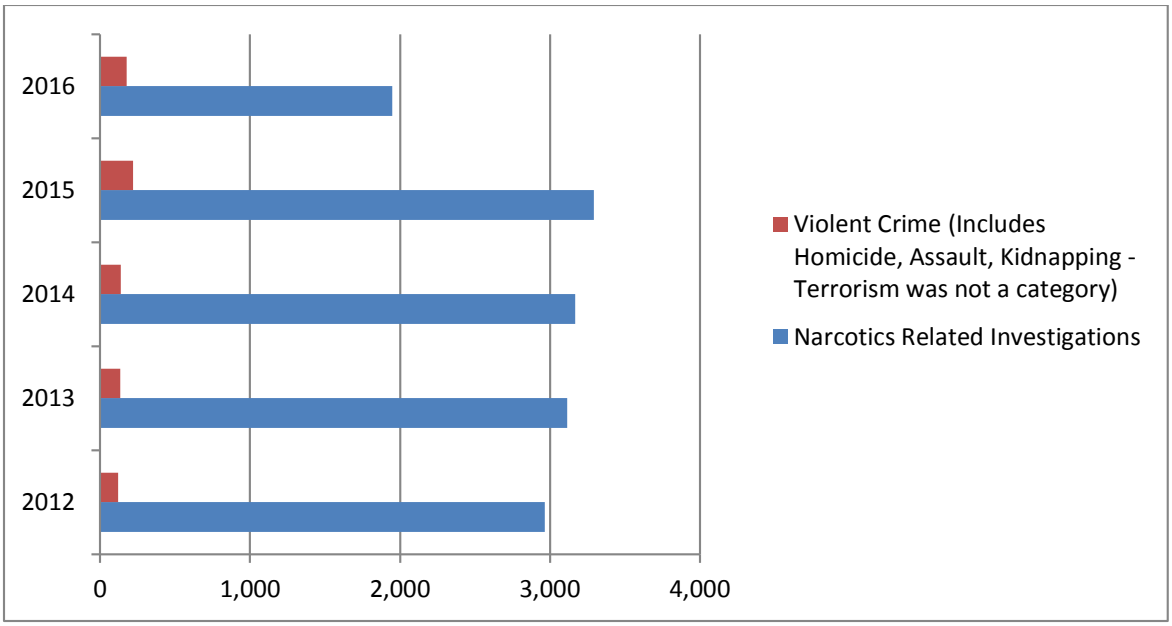

Figure 1. Title III Intercept Crime Statistics[301]

E. A FAILURE TO COMMUNICATE

The FBI's former director and general counsel have raised the issue of the "Going Dark" problem and have stated that criminals and terrorists can exploit these encrypted communication platforms to engage in nefarious activity.[302] Judiciary House Representative Henry Johnson, Jr. labeled the protections that these platforms provide as a "zone of impunity."[303] Representative Trey Gowdy lamented that Apple has commandeered legislative authority by creating devices and encryption that are immune to warrants and other legal process.[304] New York DA Cyrus Vance, Jr., voiced his concern that Silicon Valley companies have placed themselves in the position to decide what is best for the public, instead of elected officials.[305] DA Vance provided anecdotal evidence that criminals are aware of enhanced encryption and are exploiting it for

[301] Source: United States Courts, "Wiretap Reports."

[302] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 5–6; H.R., *Encryption Tightrope*, 52.

[303] H.R., *Encryption Tightrope*, 52.

[304] Ibid., 56.

[305] Ibid., 134.

criminal purposes.[306] Conversely, privacy experts claim that fast-paced innovation and early user adoption have provided law enforcement with numerous options for data collection.[307] Many tout the government's ability to obtain metadata as a law enforcement windfall.[308] Although, communication content is not included in this information, privacy experts claim that if appropriately analyzed, law enforcement can link subjects in a conspiracy and determine patterns of life.[309] However, if such cases proceed to the trial phase, more information would likely be required for evidentiary purposes. Without message content or voice recordings, a subject would be able to claim that someone else was in possession of their device and used it without their knowledge. In addition, content would be required to determine terrorist plot specifics. Privacy experts have called on the government to publicly define investigative needs and hurdles.[310] However, doing so would force law enforcement to tip its investigative hand, allowing criminals and terrorists alike to gain insight and adjust their practices accordingly. Privacy experts believe that if law enforcement is not forthcoming with this information, then the situation must not be all that dire.[311] The lack of timely prosecutorial reporting whether justified or not, does little to help the government's cause in enlisting the help of the private sector. However, a problem is unlikely to be solved if the public and their elected representatives are unaware of the seriousness of the issue. This seems to be an additional area where existing policy falls short.

306 H.R., *Encryption Tightrope*, 131; Greenblatt and Cribb, "Encrypted Evidence."

307 Swire and Oliver, "The Golden Age."

308 Ibid.

309 Ibid.

310 Abelson et al., "Keys under Doormats," 3–4.

311 Conor Friedersdorf, "Is Law Enforcement Crying Wolf about the Dangers of Locked Phones?" *Atlantic*, February 19, 2016, https://www.theatlantic.com/politics/archive/2016/02/is-law-enforcement-crying-wolf-about-the-dangers-of-locked-phones/470055/.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ENCRYPTION AND DECRYPTION METHODS

The first section of this chapter focuses on the various enhanced encryption methods currently available to safeguard devices, which also have the effect of creating roadblocks for law enforcement in its efforts to access communication content. The second section of this chapter focuses on the possible decryption techniques that law enforcement could employ to capture electronic communications in furtherance of investigations. Theoretically, some of these options have the potential to solve the going dark issue by compelling the private sector to assist law enforcement, or by allowing law enforcement to bypass, but not inhibit, the use of enhanced encryption through new methods. Three former senior officials from the National Security Agency (NSA), the Department of Homeland Security (DHS), and the Department of Defense (DOD) assert that enhanced encryption protects the nation, its citizens, and businesses and should not be compromised for the sake of law enforcement.[312] These senior officials posited that law enforcement was resourceful and through adaptation and innovation would find a solution to this issue.[313] Many of the options detailed below have been proposed in the past, but to date privacy experts and technology companies have yet to agree on a solution.

A. ENHANCED ENCRYPTION

This section analyzes the various forms of enhanced encryption. One method, known as forward secrecy, provides strong protection against intrusion by creating fresh keys for every process.[314] Device content remains incomprehensible until the passcode is

[312] Michael Chertoff, Mike McConnell, and William Lynn, "Why the Fear over Ubiquitous Data Encryption Is Overblown," *Washington Post*, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html?utm_term=.fae580e2b4c7.

[313] Ibid.

[314] House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group Year End Report* (Washington, DC: House Judiciary Committee & House Energy and Commerce Committee, 2016), 2, http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/documents/114/analysis/20161219EWGFINALReport_0.pdf.

keyed when full-disk encryption is employed.[315] When end-to-end encryption is used, message content is unreadable until it reaches the intended recipient's device.[316] Another option, symmetric encryption, introduces a code into the message that decrypts the content, but this method is not without risk.[317] Lastly, asymmetric encryption creates keys to encrypt and decrypt message content.[318] However, this form of encryption carries with it a practical limitation.[319] What follows is a detailed explanation of the known enhanced encryption techniques currently in use.

1. Forward Secrecy

Unique encryption keys are created for every operation the device processes when forward secrecy is employed.[320] Therefore, if a bad actor were to gain access to a device, then only the data from the time of the intrusion would be jeopardized.[321] Encryption of earlier data would stay intact and any operations occurring after the breach would also be protected.[322] A further precaution designed in forward secrecy is the erasure of keys following every operation.[323] Similarly, authenticated encryption, which assures privacy and confirms a message has not been altered, may not be widely used if it becomes known that vulnerabilities have been added.[324] Privacy experts also argue that

315 Potapchuk, "A Second Bite at the Apple," 1404, 1409.

316 Andy Greenberg, "Hacker Lexicon: What Is End-to-End Encryption?" Wired, November 25, 2014, https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

317 "Description of Symmetric and Asymmetric Encryption," Microsoft Support, accessed February 5, 2017, https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption.

318 Ibid.

319 Ibid.

320 House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group*, 2.

321 Ibid.

322 Ibid., 2, 3.

323 Ibid., 3.

324 Abselson et al., "Keys under Doormats," 2.

engineering devices with backdoors or vulnerabilities would endanger innovation and inhibit the widespread adoption of forward secrecy.[325]

2. Full-Disk Encryption

Apple's iOS 8 defaults to full-disk encryption.[326] According to an Apple iOS Security white paper from March 2017:

> iOS and iOS devices provide advanced security features, and yet they're also easy to use. Many of these features are enabled by default, so IT departments don't need to perform extensive configurations. And key security features like device encryption aren't configurable, so users can't disable them by mistake.[327]

Until the correct password is keyed, full-disk encryption makes all data on the device indecipherable.[328] If a user's device falls into the hands of a third party, full-disk encryption prevents the third party from accessing the stored data.[329] Some users may experience negative consequences due to the deployment of full-disk encryption. If a user forgets his/her passcode and has not backed up data, the information stored on the device will likely be irretrievable.[330] However, if customer data was backed up to a cloud storage system, they may be able to restore their historical data.[331] As Apple, Google and other companies are intentionally removing themselves from the access equation, they are limiting their customer's choices and the ability to assist them, as well as law enforcement.

---

[325] House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group*, 2.

[326] Potapchuk, "A Second Bite at the Apple," 1410–1411.

[327] Apple, *iOS Security* (Cupertino, CA: Apple, 2017), 4, https://images.apple.com/business/docs/iOS_Security_Guide.pdf.

[328] Potapchuk, "A Second Bite at the Apple," 1404, 1409.

[329] Kim Zetter, "Hacker Lexicon: What Is Full Disk Encryption?" Wired, July 2, 2016, https://www.wired.com/2016/07/hacker-lexicon-full-disk-encryption/.

[330] Apple, "Apple Will No Longer Unlock"; "If You Forgot the Passcode for Your iPhone, iPad, or iPod Touch, or Your Device Is Disabled," Apple Support, December 18, 2017, https://support.apple.com/en-us/HT204306.

[331] Ibid.

3. End-to-End Encryption

Another technique used to protect data is end-to-end encryption. End-to-end encryption ensures that once a message is sent, it remains encrypted until it reaches the intended recipient.[332] The intended recipient's device has the only key capable of decrypting the message. The message cannot be intercepted and decrypted in-transit.[333] The server used to carry the message from the sender to the recipient acts as a transporter only and cannot read the communications.[334]

4. Symmetric Encryption

A commonly used method to secure communications is symmetric encryption, also referred to as secret key encryption.[335] Users of symmetric encryption insert an alpha-numeric combination into the communication to modify the content.[336] Through the use of this secret key, the sender and the recipient can encrypt and decipher their communications.[337] However, the secret key is vulnerable if one of the parties falls prey to hackers.[338]

5. Asymmetric Encryption

Some devices have programs installed that use an algorithm to create a unique set of keys.[339] These keys are known as asymmetric or public/private keys.[340] The private key is safeguarded, and the public key can be shared with any user.[341] Encrypting a

---

[332] Greenberg, "Hacker Lexicon."

[333] Ibid.

[334] Ibid.

[335] "Description of Symmetric and Asymmetric Encryption," Microsoft Support, accessed February 5, 2017, https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption.

[336] Ibid.

[337] Ibid.

[338] Ibid.

[339] "Asymmetric Keys (Windows)," Microsoft Developer Network, accessed February 5, 2017, https://msdn.microsoft.com/en-us/library/windows/desktop/aa387460(v=vs.85).aspx.

[340] Ibid.

[341] Ibid.

communication with one of the keys in the set requires the use of the second key to decipher the message.[342] The drawback with using asymmetric keys is the protracted processing time, approximately one-thousand times slower than symmetric key encryption, which makes them unfeasible for sizeable messages.[343]

B. DECRYPTION/ACCESS TECHNIQUES

Following is an analysis of the varying decryption techniques as well as other avenues that law enforcement may explore in the future to access electronic communications. The use of split-key encryption allows law enforcement the access it has enjoyed in the past, while providing a check and balance since two entities must work together to obtain device content.[344] Signing updates could be sent to specific devices to allow law enforcement to break passwords to access stored data or load spyware for interception purposes.[345] Germany has recently granted law enforcement the authority to install spyware on target devices to overcome the encryption issue.[346] Legal hacking, whereby the government employs individuals with the skills necessary to access the myriad communication devices and platforms currently available, is a somewhat controversial solution some privacy experts support.[347] Another option that has been suggested is compelling users to divulge their passcodes.[348] However, this method brings

---

[342] Microsoft Developer Network, "Asymmetric Keys (Windows)."

[343] Ibid.

[344] Schaul, "Encryption Techniques."

[345] Peter Bright, "Encryption Isn't at Stake, The FBI Knows Apple Already Has the Desired Key," Ars Technica, February 18, 2016, https://arstechnica.com/apple/2016/02/encryption-isnt-at-stake-the-fbi-knows-apple-already-has-the-desired-key; Andrea Peterson and Ellen Nakashima, "Obama Administration Explored Ways to Bypass Smartphone Encryption," *Washington Post*, September 24, 2015, https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html.

[346] *Homeland Security Newswire*, "Growing Opposition in Germany."

[347] Susan Landau, "The Real Security Issues of the iPhone Case, Law Enforcement Needs 21st-Century Investigative Savvy," *Science* 352, no. 6292 (June 17, 2016): 1398–1399; House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group*, 11; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 8.

[348] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 8.

up Fifth Amendment issues.[349] Others have recommended that law enforcement rely on data that has been stored in the cloud to meet its investigative needs, but this process has not yet been widely adopted and those who do employ it may not do so with any regularity.[350] When key escrow is employed, an extra key is created that could be held by the device designer or law enforcement in the event access to content is necessary.[351] Finally, some experts believe that the Internet of Things will provide law enforcement with new intercept techniques that will compensate for its current inability to access certain devices.[352] A detailed discussion of these techniques follows.

1. Split-Key Encryption

Split-key encryption would prevent any one entity from gaining access to a device.[353] This method requires the key to be divided into at least two parts, depending on the number entities involved, so that no one entity would be able to unilaterally decrypt content.[354] Theoretically, successful decryption would require the collaboration of two or more parties, such as the FBI and Apple.[355] In this example, the FBI would obtain and serve Apple with proper legal process. Apple would then work with an FBI representative and each entity would use their portion of the key to access the device and decrypt the data.[356] This lessens the likelihood that a single organization would be vulnerable to hackers seeking a specific key.[357] As the key is split, hackers would have to successfully infiltrate two organizations.[358] The Director of the NSA, Michael Rogers, is

---

[349] Potapchuk, "A Second Bite at the Apple," 1414.

[350] Federal Bureau of Investigation, "Encryption and Cyber Security for Mobile Electronic Communication Devices"; Crowley and Johnstone, "Protecting Corporate Intellectual Property," 626.

[351] Abelson et al., "Keys under Doormats," 5.

[352] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 13–15.

[353] Schaul, "Encryption Techniques."

[354] "Key Management: A Cryptography Tutorial," Cryptography World, accessed January 23, 2017, http://www.cryptographyworld.com/key.htm.

[355] Schaul, "Encryption Techniques."

[356] Ibid.

[357] Abselson et al., "Keys under Doormats," 2.

[358] Schaul, "Encryption Techniques."

a proponent of the split-key option.[359] This method protects against the insider threat posed by private sector employees and the potential abuse of authority by government entities.[360] This collaboration may also have the added benefit of fostering closer associations between the government and corporations.

2. Signing Updates

Some providers, including Apple, use signing updates to push out system updates including the latest operating system or security patches to their customers.[361] Apple devices, for instance, default to automatic updates for users employing the most current operating systems.[362] Updates automatically download in the background then users receive a message informing them that an update is available.[363] Apple gives the user two options at this stage: "Install Now" or "Remind Me Later."[364] Therefore, unless the user takes steps to disable this feature, automatic updates will occur when the device is plugged in and the user selects one of the installation options.[365] This process could also be used to load a different operating system onto a device that would allow law enforcement to mount a brute-force attack.[366] A brute-force attack is one in which law enforcement uses specially designed computer programs to attempt to break the device's password and gain access by rapidly trying a series of passwords until one is found that works.[367] The signing update could be specifically designed to remove the rate-limiting feature. Rate-limiting is a feature designed to prevent brute-force attacks, as it requires a

---

[359] Nicole Perlroth, "Security Experts Oppose Government Access to Encrypted Communication," *New York Times*, July 7, 2015, http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html.

[360] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 16.

[361] Lucy Hattersley, "How to Stop iPhone from Asking to Update to the Latest Version," *Macworld UK*, July 6, 2016, http://www.macworld.co.uk/how-to/iphone/how-stop-ios-nagging-you-update-latest-version-3641478/; Landau, "The Real Security Issues," 1398–9.

[362] Ibid.

[363] Ibid.

[364] Ibid.

[365] Ibid.

[366] Finklea, Thompson, and Jaikaran, *Court Ordered Access to Smartphones*, 2.

[367] Bright, "Encryption Isn't at Stake."

certain period of time to lapse before additional password attempts can be made.[368] This makes the process time-prohibitive for law enforcement.[369] Further, many devices have features that remove all useful data if too many unsuccessful password attempts are made.[370] Signing updates could also be used to load spyware onto a device so that law enforcement, armed with proper legal process, could monitor the device.[371] However, those opposed believe it would encourage consumers to avoid updates, placing their privacy at risk.[372]

3. Germany's State Trojan

Germany is taking a new approach to combatting the encryption issue that employs a hybrid of the signing updates and legal hacking options. As the result of multiple terrorist attacks that have plagued Europe, German lawmakers voted in June 2017 to help law enforcement gain access to encrypted communications.[373] Germany reported that 85% of the country's communications are encrypted.[374] These factors combined were the impetus behind the Bundestag passing this legislation, known as the Source Telecommunications and Online Surveillance Law, to help law enforcement bridge the gap created when communication providers and device designers began engineering their products with enhanced encryption.[375] Effective July 1, 2017, German authorities have been granted authority to install spyware, known as a State Trojan, onto target devices when armed with proper legal process.[376] This technique allows law enforcement to collect the content of messages in real time, and view the messages just as

368 Steve Mansfield-Devine, "The Battle for Privacy," *Network Security*, June 2016, 12.

369 Ibid.

370 Bright, "Encryption Isn't at Stake."

371 Peterson and Nakashima, "Obama Administration Explored Ways to Bypass Smartphone Encryption."

372 Ibid.

373 "Growing Opposition in Germany to New Surveillance Measures," *Homeland Security Newswire*, June 26, 2017, http://www.homelandsecuritynewswire.com/dr20170626-growing-opposition-in-germany-to-new-surveillance-measures.

374 "Stenograph Record, 240th Session, Plenary 18/240," German Bundestag, June 22, 2017, 24592.

375 Chase, "Things to Know"; Bleiker, "New Surveillance Law."

376 *Homeland Security Newswire*, "Growing Opposition in Germany."

the intended recipient would.[377] Installing the State Trojan permits law enforcement to see the message before it is sent and more importantly before it is encrypted.[378] The State Trojan may also be installed on the recipient's device that would enable law enforcement to intercept the message once it has been decrypted by the user's device.[379] This new legislation also authorizes law enforcement to access stored content on individual devices or systems.[380]

The passage of this law is remarkable considering how staunchly protective Germany is of individual privacy rights.[381] For decades, East German citizens were subjected to continuous and overreaching surveillance by the Stasi.[382] This surveillance included the most intimate details of innocent citizens' lives.[383] During this time, the Stasi reportedly maintained records on one-third of the population.[384] German citizens were also among the most outspoken against the NSA's activities following Snowden's revelations.[385] However, outrage against these episodes may have been overshadowed by the four terrorist attacks the country suffered in 2016 alone.[386] Lawmakers may have realized that guarding these rights may be in direct conflict with law enforcement's goals and responsibilities, which provided the traction necessary for ratification.[387] Nevertheless, this law is not without controversy and was opposed by Greens party

---

377 Bleiker, "New Surveillance Law."

378 "18 Election Period 12785," German Bundestag, 49, June 20, 2017, https://translate.google.com/translate?hl=en&sl=de&u=http://dip21.bundestag.de/dip21/btd/18/127/1812785.pdf&prev=search.

379 Ibid.

380 Bleiker, "New Surveillance Law."

381 "Germany Expands Surveillance of Encrypted Message Services," Phys Org, June 22, 2017, https://phys.org/news/2017-06-germany-surveillance-encrypted-message.html.

382 Joel D. Cameron, "Stasi East German Government," *Encyclopaedia Britannica*, April 11, 2016, https://www.britannica.com/topic/Stasi.

383 Ibid.

384 Ibid.

385 "Thousands of Germans Rally to End Government Spying," RT News, August 31, 2014, https://www.rt.com/news/184000-berlin-protests-surveillance-government/.

386 "Timeline of Recent Terror Attacks in Western Europe," *Newsweek*, April 8, 2017, http://www.newsweek.com/timeline-recent-terror-attacks-western-europe-580977.

387 German Bundestag, "18 Election Period 12785," 48.

members and those on the far left.[388] At this time, it is unknown if the device user/target would be aware that the spyware has been inserted, and therefore alerted to law enforcement's actions. As the results of this method remain untested, at least publicly, it is possible that the initial loading of the spyware could result in slower device response times, which could present a red flag to the device user/target. However, after the installation process is complete, any impeded device performance may return to normal. Passage of this law in Germany may increase the chances that it will be modeled in other countries, especially if it can be demonstrated that it has been effective in preventing a terrorist attack or capturing co-conspirators, without unduly threatening the privacy of innocent citizens.

4. Legal Hacking

Privacy experts have suggested that law enforcement should invest in creating laboratories and hiring individuals with the skills necessary to access devices.[389] They point to the FBI's ability to find a third-party who provided them with access to the San Bernardino terrorist's device.[390] However, this so-called legal hacking is not without controversy. If the government is able to attract individuals with the knowledge and skills to hack devices, will they be able to pass law enforcement's stringent background investigations, which are a requirement for the hiring process? Most state, local and tribal agencies lack the funding necessary to build and staff suitable laboratories.[391] These agencies also lack the funding to farm out devices to third-party vendors to infiltrate on a case-by-case basis.[392] In addition, most government wages do not compare with those offered in Silicon Valley. More importantly, if these individuals become government employees and uncover vulnerabilities in specific device designs, is there a moral or legal

---

[388] Phys Org, "Germany Expands Surveillance."

[389] Landau, "The Real Security Issues," 1398–1399.

[390] Ibid.

[391] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 30.

[392] Ibid.

obligation to notify the company of the weaknesses?[393] To do so would allow the company to fix any weaknesses and therefore protect its customers and intellectual property.

But this would come at a cost to law enforcement. Law enforcement would have to return to the drawing board to identify a new vulnerability that would provide access for any future devices of the same model, as the uncovered weaknesses would no longer exist. It seems unlikely that legal hackers would enjoy much success, as the device designers claim that they cannot break their own encryption.[394] Apple's General Counsel testified that the company would take issue with the FBI successfully hacking their devices.[395] In addition, attempting to uncover vulnerabilities for the variety of devices on the market would be extremely costly and time-consuming, and in some cases, time is not a luxury that law enforcement is afforded.[396] Moreover, data obtained through hacking would be challenged in court when cases progress to the trial phase, as this method is untested.[397] At question would be data integrity, specifically whether law enforcement planted evidence or omitted exculpatory evidence.[398] Tying up cases in the judicial system would unnecessarily cost taxpayers money and law enforcement time, all of which could have been avoided if providers continued to supply law enforcement with trusted device content.[399] This option seems like a better fit for the NSA, as opposed to state, local and federal law enforcement, which have limited resources.

---

[393] House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group*, 11.

[394] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 30.

[395] H.R., *Encryption Tightrope*, 168.

[396] House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group*, 11.

[397] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 8.

[398] Ibid.

[399] Ibid.

5. Compelling Users to Reveal Their Passcodes

Some technology companies have also suggested that law enforcement should compel device holders to reveal their passwords.[400] This solution is not feasible as it would jeopardize ongoing investigations. An argument can also be made that forcing an individual to divulge information that may ultimately be used against that person in a court of law violates the Fifth Amendment.[401] In the case of the San Bernardino terrorists, the device users were deceased, making the point moot.[402] However, in instances where investigations are not in the covert stage and law enforcement has access to the subjects and their devices, some targets have been compelled to disclose passcodes or use their fingerprints to unlock devices.[403] Judicial rulings have varied depending on the state.[404] A Florida judge ruled that compelling a subject to reveal his/her passcode is not protected by the Fifth Amendment, while judges in Pennsylvania and Colorado disagreed.[405] Apple iOS 11, which is slated to be released in the fall of 2017, will reportedly have a function that allows the user to disable the Touch ID sensor feature by engaging the power button five times.[406] When Touch ID is enabled, the user's fingerprint is used for authentication purposes to unlock the device.[407] Some are referring to this new feature as the "cop button" because they anticipate it will thwart law enforcement's ability to quickly and easily access user devices and content.[408]

---

400 Potapchuk, "A Second Bite at the Apple," 1414.

401 Ibid.

402 Deirdre Mulligan and Nick Doty, "Design Wars: The FBI, Apple and Hundreds of Millions of Phones," *UC Berkeley* (blog), March 3, 2016, http://blogs.berkeley.edu/2016/03/03/design-wars-the-fbi-apple-and-hundreds-of-millions-of-phones-3/.

403 Alison DeNisco Rayome, "Police Can Force You to Give up Your iPhone Password, Florida Court Rules," TechRepublic, December 20, 2016, http://www.techrepublic.com/article/police-can-force-you-to-give-up-your-iphone-password-florida-court-rules/; David Meyer, "Will Apple's iOS 11 'Cop Button' Help Protect iPhone Privacy?" *Fortune*, August 17, 2017, http://fortune.com/2017/08/18/apple-ios-11-cop-button-iphone-ipad-privacy/.

404 Rayome, "Police Can Force You to Give up Your iPhone Password."

405 Ibid.

406 Meyer, "Will Apple's iOS 11 'Cop Button' Help Protect iPhone Privacy?"

407 Ibid.

408 Ibid.

6. Access via Cloud Storage

Backing up data to the various cloud systems provides unlimited storage capacity and convenience, but the process is not without vulnerabilities. Companies that offer cloud storage, such as Microsoft, Dropbox and Google, all allow mechanized processes, employees, and some third parties to view data.[409] These policies place individual privacy and the intellectual property of those entrusting their data storage to the cloud at risk.[410] Consumers can take precautions, such as employing zero-knowledge technology.[411] Prior to uploading the information to the cloud, the user encodes the message, which in theory would mean that only the user can access the data.[412] However, this is done with a level of trust that no backdoors have been built into the software.[413] Users have the option of obtaining their own encryption software rather than using what is provided by the cloud administrator.[414] Some technology companies claim that law enforcement should turn its focus to serving cloud storage companies with proper legal process to obtain the data it needs for investigations.[415] However, not every user backs their data up in this method.[416] Reasons for this vary, including associated service fees, lack of trust in security protocols, or underestimating the value of device backup.[417] In the case of the San Bernardino terrorists, the saved data was not relevant because it had not been backed up for six weeks.[418] In addition, if zero-knowledge or other enhanced encryption is used, then data stored in the cloud will remain out of law enforcement's reach.

---

409 Crowley and Johnstone, "Protecting Corporate Intellectual Property," 627.

410 Ibid., 627–628.

411 Ibid.

412 Ibid.

413 Ibid.

414 Ibid.

415 Federal Bureau of Investigation, "Encryption and Cyber Security."

416 Ibid.

417 Ibid.

418 Crowley and Johnstone, "Protecting Corporate Intellectual Property," 626.

7. Key Escrow

Another possibility that may provide law enforcement with the assistance it requires is the use of key escrow.[419] In the event future access is warranted, key escrow creates an additional symmetric key that would be in the possession of the device creator or the government.[420] Public keys for the intended recipient and the escrow agent would be included with every message sent.[421] The symmetric key could be decrypted by the escrow key, allowing for the data to be deciphered.[422] The argument against this approach is that it would encourage hackers to actively infiltrate the escrow entity.[423] However, hackers would have to know that this method was in use and which entities acted as escrow agents. Technology experts claim that insiders could exploit the system if key escrow were employed.[424] Yet Apple maintains encryption keys to access data stored in the cloud, which begs the question, why is it safe enough for the cloud but not phones? Apple's General Counsel responded to this query following testimony provided in March 2016.

> Securing data that exists on servers in apple's facilities is a very different challenge from securing data that exists on an iPhone or an iPad in the possession of our customers. These devices are physically lost and stolen. In addition, customers use iCloud in different ways from how they use their devices, so in designing our products we take those differences into account. This is a question that we continually address as we strive to make our products both as secure and as usable as possible.[425]

8. Internet of Things

Experts claim that with the advent of the IoT, common household appliances will replace commonly used communication methods that can be exploited to eavesdrop on

---

419 Schaul, "Encryption Techniques."

420 Abselson et al., "Keys under Doormats," 5.

421 Ibid.

422 Ibid.

423 Schaul, "Encryption Techniques."

424 Finklea, Thompson, and Jaikaran, "Court-Ordered Access to Smart Phones," 6.

425 H.R., *Encryption Tightrope,* 190.

private conversations in a subject's home.[426] However, these technologies have yet to be widely adopted, and would necessitate arming law enforcement with the knowledge of specific devices used. Even if and when these IoT devices become more commonly used, their reliability is in question and this type of electronic surveillance has not been tested in court. How would minimization be accomplished in order to protect innocent parties and judicially recognized privileges, such as between spouses, clergy/parishioner, doctor/patient, and attorney/client?[427] In addition, in life or death investigations, there is no guarantee that a household appliance would pick up conversations detailing where and when an attack is planned, or where a kidnapping victim is being held.

Many possibilities currently exist, and others could be specifically created to allow law enforcement to continue accessing electronic communications regarding investigative targets. The challenge lies is determining which, if any, of the possible solutions detailed above will meet the needs of law enforcement without compromising individual privacy or the intellectual property of communications providers and device creators. Is it possible to find common ground on this issue between the interested parties? Are communication technologies and encryption capabilities evolving so rapidly as to make any proposed solution improbable?

C. ANALYSIS OF DECRYPTION/ACCESS TECHNIQUES

The varying techniques available to law enforcement are further analyzed in Table 3. Each decryption/access technique was examined to determine viability, risk and potential costs that may cause concern for privacy experts, law enforcement and legislators. The categories scrutinized were based on objections that the various stakeholders have raised throughout the debate on this topic. Scores were assigned by entity impact, with higher scores equating to increased risk and/or costs.

---

[426] Berkman Center for Internet & Society at Harvard University, "Don't Panic," 13–15.

[427] "Legal Definition of Privileged Communication," Lectric Law Library, accessed June 16, 2017, http://www.lectlaw.com/def2/p084.htm.

Table 3. Policy Options Matrix-Weighted Comparison of the Varying Decryption/Access Techniques

Technique	Hacking Risk	Corporate Protection/Control	Corporate Burden (Includes Costs, Staffing)	Likely to be Challenged in Court (Evidence Planted, Exculpatory Evidence Omitted)	Government Costs	Government Obligations	Misc. Issues	Score
Internet of Things (IoT)	High (3)	Medium (2)	Medium (2)	High (3)	Medium (2) (Cost of new technology, training, learning curve, to intercept myriad of devices)	High (3) (Ensuring innocent parties are not intercepted, privileges protected)	High (3) (Untested; Not widely adopted)	18
Key Escrow	Medium (2) (A single entity may be targeted: outside hackers or rogue insider)	High (1)	Medium (2)	Low (1)	Low (1)	Medium (2) (Collaboration with private sector would depend on whether or not the government holds keys in escrow)	Low (1) (Could be delay in receiving data if provider holds sole key)	10
Legal Hacking	(0)	None (3)	None (0)	High (3)	High (3) (Includes both financial costs for training hackers and equipping and maintaining labs, Time spent hacking new devices, What happens if device cannot be penetrated?, Potential damage to image due to negative connotation of hacking)	High (3) (Notifying tech companies of vulnerabilities)	High (3) (Not feasible for most state, local and many federal law enforcement agencies; Better suited to NSA)	15
Signing Updates	Low (1)	High (1)	Medium (2)	Medium (2)	Low (1)	Low (1) (Collaboration with private sector)	Medium (2) (Users can opt out of updates)	10
Split-Key Encryption	Low (1)	Medium (2)	Medium (2)	Low (1)	Low (1)	Low (1) (Collaboration with private sector)		8
State Trojan/Spyware Insertion	Low (1)	Medium (2)	None (0)	Medium (2)	Low (1) (Cost of modifying existing technology, training)	Medium (2) (Abide by minimization rules - More controlled than IoT)	Low (1) (Untested)	9

The results of the analysis indicate that some of the techniques do not seem viable as the cost or risk level is too high. The IoT is untested and it is unknown if any of the devices with the potential to be exploited were designed in a manner to prevent such activity. As a result, whether this method could successfully be used to collect useable information that would withstand judicial scrutiny is questionable. Key escrow would likely still require the assistance of the private sector that would bear the brunt of the costs, and be vulnerable to outside hackers and rogue insiders. Law enforcement may also experience delays in receiving data depending on the provider's timetable. Legal

hacking would require a significant capital outlay for the government, which would make it cost prohibitive for state and local law enforcement. Isolating exploitable vulnerabilities for the myriad devices and operating systems on the market would be extremely time-consuming and present a moral dilemma as to whether law enforcement would be obligated to notify providers of any identified weaknesses. Signing updates may afford defense attorneys the opportunity to suggest that evidence was planted or exculpatory evidence was omitted. In addition, the private sector would bear the burden of costs, and users can opt out of updates that would render this method ineffective. However, the analysis also revealed that there were two options that may be feasible, split-key encryption and spyware insertion.

1. Split-Key Encryption Advantages and Disadvantages

Using the analysis in the table above, split-key encryption presents a promising option. As two or more keys are required to decrypt communications, the risk of outside hacking is significantly diminished. Device designers would be able to safeguard their intellectual property and protect customer privacy from insider threats by sharing decryption responsibilities with law enforcement. Although the private sector would bear the brunt of the costs, engineering this option in the design phase would save device designers money and law enforcement time, with the added benefit of potentially reducing vulnerabilities.[428] Split-key encryption would also likely withstand legal challenges in the event an investigation proceeds to the trial phase, unlike the untested options of signing updates, legal hacking and the exploitation of the IoT. These methods open the door for defense attorneys to claim that law enforcement planted incriminating evidence, omitted exculpatory evidence, or did not adequately protect judicially recognized privileges. The collaboration necessary for the split-key option provides a system of checks and balances, reducing the chances for either party to introduce or modify data and content. The cost to the government would likely be the same as for any Title III intercept, unlike the considerable costs of purchasing equipment and hiring personnel to establish legal hacking laboratories. Many state, local, and federal agencies

[428] Hibbard, "Wiretapping the Internet," 396.

lack funding for such an endeavor. Finally, the required collaboration may improve the relationship between the public and private sectors.

Drawbacks to split-key encryption include the requirement for new or amended legislation to compel compliance. This could prove difficult as the private sector's willingness to assist law enforcement has diminished significantly since the Snowden leaks.[429] In addition, technology firms have the resources to employ lobbyists whose responsibility it is to ensure that their best interests are considered by lawmakers.[430] Lastly, most device designers and communication providers do not assist law enforcement free of charge. Many companies charge by the type of assistance provided, such as specified fees for Title III intercepts, or by the time spent replying to other law enforcement requests.[431] Additionally, there can be considerable lags in response times, depending on the type of request.

2. Spyware Insertion Advantages and Disadvantages

Conversely, the legislation that German lawmakers recently enacted allowing authorities to insert spyware onto a target's device may also prove to be a viable option.[432] Although this technique is still in its infancy, it does not seem to be overly costly or place the public or corporate intellectual property at undue risk. This technique appears to be similar to how French authorities have examined target computers since 2011. Prior to adopting this option, U.S. lawmakers, as well as law enforcement could reach out to their German and French counterparts to determine the effectiveness of these methods and make amendments to any proposed legislation based on lessons learned. A major concern of privacy and security experts has been that providing law enforcement backdoor access would endanger technological ingenuity and discourage the public from

---

[429] Susan Hennessey and Benjamin Wittes, "Apple Is Selling You a Phone, Not Civil Liberties," *Lawfare* (blog), February 18, 2016, https://www.lawfareblog.com/apple-selling-you-phone-not-civil-liberties.

[430] Hamza Shaban, "At the Start of the Trump Era Facebook and Apple Spent More on Lobbying than Ever," CNBC, April 21, 2017, https://www.cnbc.com/2017/04/21/at-the-start-of-the-trump-era-facebook-and-apple-spent-more-on-lobbying-than-ever.html.

[431] "Verizon, AT&T Get Most Bucks from Feds for Wiretaps," CBS News, July 11, 2013, https://www.cbsnews.com/news/verizon-att-get-most-bucks-from-feds-for-wiretaps/.

[432] *Homeland Security Newswire*, "Growing Opposition in Germany."

employing encryption to protect individual privacy.[433] Device designers and communication providers are not being directed to modify their products in order for the spyware to be inserted; therefore it is arguable as to whether this method constitutes a backdoor.

The value of this option lies in its simplicity and may have the added benefit of saving law enforcement the time and expense of continually adapting to new and ever more sophisticated encryption techniques. As the spyware gives authorities access to message and device content prior to encryption or after decryption, it follows that law enforcement will not be hamstrung by future encryption developments.[434] The deployment of the State Trojan technique has the potential to save lives if information regarding future terrorist attacks can be extracted from messages that have been placed out of law enforcement's reach by enhanced encryption and the private sector's desire to use privacy and anonymity as marketing tools for their products.[435] Additionally, it does not appear that this option requires the cooperation of the private sector.

After reviewing the various potential options for restoring law enforcement's access to electronic communications, two techniques stand out as being the most feasible: split-key encryption and the insertion of State Trojans. These options appear to provide the most protection to individual privacy and corporate intellectual property, as well as being cost-effective. However, split-key encryption relies on collaboration with the private sector, which has openly opposed assisting law enforcement overcome encryption issues. Although the installation of spyware would likely be challenged in court proceedings, installing State Trojans seems more controlled than the aforementioned legal hacking. Analyzing Germany's successes and/or failures with this option in January 2018 may prove useful. It may be prudent to scrutinize the State Trojan's effectiveness and any legal ramifications that may have surfaced after this technique has been in use

[433] House Judiciary Committee & House Energy and Commerce Committee, *Encryption Working Group*, 2.

[434] German Bundestag, "18 Election Period 12785," 49.

[435] Apple, *Legal Process Guidelines*; Timberg, "Newest Androids."

for six months. This analysis may aid U.S. lawmakers in crafting appropriate legislation if it is deemed a viable option.

V. CONCLUSION AND RECOMMENDATIONS

Capturing and analyzing communications has long been an effective tool in law enforcement's arsenal. This capability has aided in the furtherance of countless investigations and many public safety agencies consider it invaluable. CALEA is the primary legislation used to compel communication providers to assist law enforcement with intercepting traditional telephone and VoIP communications.[436] However, continuous innovation has led to the advent of new methods of communication, which are not subject to the mandates of CALEA.[437] Further, following the Edward Snowden leaks, many in the technology field began engineering their products and devices with enhanced encryption.[438] The rationale for these changes was to safeguard individual privacy, as well as corporate intellectual property.[439] However, both the emergence of new communication platforms that are not legislated by CALEA, and the addition of sophisticated encryption that in many cases law enforcement has been unable to bypass, have had a detrimental impact on criminal and terrorist investigations.[440]

The enhanced encryption that companies, such as Apple and Google have engineered into their products is so sophisticated that even when served with proper legal process, they themselves cannot bypass it to assist law enforcement.[441] Despite the best intentions of the device designers, negative consequences arise from enhanced encryption. Investigative targets seek out methods of communications that provide anonymity, and if law enforcement is unable to access communications, then the criminal element benefits from these enhancements.[442] The difficulty lies in providing law

---

[436] Federal Communications Commission, "Communications Assistance for Law Enforcement Act."

[437] Hibbard, "Wiretapping the Internet," 372–373.

[438] Timberg, "Newest Androids."

[439] Tim Cook, "A Message to Our Customers," Apple, 623, February 16, 2016, https://www.apple.com/customer-letter/; Crowley and Johnstone, "Protecting Corporate Intellectual Property."

[440] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 8–11, 21.

[441] Cook, "A Message to Our Customers"; Timberg, "Newest Androids."

[442] H.R., *Encryption Tightrope*, 131.

enforcement with the continued access it has legislatively been granted for decades, without sacrificing individual privacy and endangering intellectual property.

Options exist for amending CALEA to include emerging communication platforms, or drafting entirely new legislation that would require providers and device designers to maintain the capability to bypass any encryption they create.[443] However, resistance has been met on many sides. Some legislators oppose requiring the private sector to comply with more stringent regulations, and the Departments of State and Commerce worry that hostile regimes could bypass encryption and persecute citizens.[444] Technology and privacy experts claim that providing law enforcement with the assistance it requires threatens innovation, international corporate sales and the privacy of all device users.[445] Many of these same experts also assert that the emerging platforms should not fall under CALEA, as users tend to communicate more freely and share more intimate details of their lives than on standard voice communications.[446]

However, the private sector has a role in safeguarding national security, and corporations benefit from operating in a stable environment.[447] As government entities, law enforcement agencies appear to be paying the price for the actions of the NSA and its mass collection of data.[448] Nevertheless, law enforcement should recognize its requests for continued access to communications may present a risk to individuals and corporations, depending on the method(s) used.[449] The research and analysis for this thesis focused on decryption techniques and legislative options that may be used to solve this controversial issue.

---

[443] *Congressional*, "Personal Data Encryption"; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety*, 13; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 15.

[444] Hibbard, "Wiretapping the Internet," 391; H.R., *Encryption Tightrope*, 173–174.

[445] Bankston, "It's Time to End the 'Debate'"; Hibbard, "Wiretapping the Internet," 390; Abelson et al., "Keys under Doormats," 6, 10.

[446] Hibbard, "Wiretapping the Internet," 387.

[447] Etzioni, "Apple Good Business?" 8–9.

[448] Timberg, "Newest Androids."

[449] Abelson et al., "Keys under Doormats," 10.

The goal of this thesis was to determine how law enforcement could overcome insurmountable encryption to access existing and emerging electronic communications to further investigations without compromising individual privacy and intellectual property. Research for this thesis uncovered six decryption/access techniques that could be used to address the "Going Dark" issue. The policy analysis method was used to analyze these techniques in an attempt to determine viability. The San Bernardino terrorist investigation was also reviewed to add perspective to the issue currently confronting law enforcement.

A. LIMITATIONS

The primary limitation of this thesis is the lack of information regarding spyware or State Trojan insertion, recently employed by the German government.[450] This method appears to be a viable solution for a segment of the "Going Dark" problem U.S. law enforcement currently faces, but as it is new and untested, its effectiveness remains unknown.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

Obtaining information from prosecutors as to why not all wiretap statistics are reported to the court could prove useful. Some prosecutors choose to delay reporting to protect ongoing investigations, but target specific data is not part of the data captured.[451] It may be that not all prosecutors are aware of the mandate to report this information or how the statistics are used, which could be why some of the data remains unreported. Perhaps training could help alleviate this problem. Surveying prosecutors to determine the reasons for reporting issues would be useful, but it may be unrealistic to expect legal professionals to willingly respond to such inquiries that could negatively impact their careers.

---

[450] Chase, "Things to Know"; Bleiker, "New Surveillance Law."

[451] "FAQs: Wiretap Reports," United States Courts, accessed August 21, 2017, http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports/faqs-wiretap-reports; Administrative Office of the United States Courts, *WT-2A Federal Form*.

It could also prove useful to conduct follow-up research on Germany's successes and failures with the deployment of the State Trojan technique.[452] Answers to the following questions could provide U.S. legislators with the information necessary to craft similar legislation that could be adopted domestically, as well as offer an avenue for future research:

- Has data integrity been an issue?
- How long does the process take?
- How effective has this method been in providing law enforcement with information to further criminal investigations?
- What percentage of devices was the State Trojan successfully installed and useable information retrieved?
- How long did it take long for law enforcement personnel to become subject matter experts?
- Has this process impacted device performance that was obvious to the target?
- Has this process been challenged in court? If so, did the use of this technique withstand judicial scrutiny?
- Have the legislators opposed to this law gained traction in repealing the measure, or have any successes firmly cemented its use by German law enforcement?[453]

C. CONCLUSION

The research and analysis for this thesis has culminated in five conclusions. The first conclusion is that newly drafted legislation or legislation amending CALEA is

[452] Chase, "Things to Know"; Bleiker, "New Surveillance Law."

[453] Phys Org, "Germany Expands Surveillance."

necessary to solve the "Going Dark" issue. Regardless of the decryption or access technique(s) chosen as the most feasible to address this problem, appropriate legislation will be necessary to ensure compliance by device designers and communication providers, or to grant law enforcement the authority to act on its own. As such, it is imperative that any new or amended legislation be crafted in such a way to withstand future technological innovations, so that this issue does not become a recurring problem as seems to be the case with CALEA.[454]

The second conclusion is that due to the limitations of existing legislation, the private sector has acted in a manner that constrains law enforcement's authority to conduct legal searches, even when armed with proper legal process.[455] Regardless of intention, technology innovators have created "zones of impunity," which allow criminals and terrorists to communicate freely and oftentimes anonymously, beyond law enforcement's reach.[456] The evidence presented in this paper strongly suggests that law enforcement investigations are suffering as a result of the "Going Dark" problem. Agencies have lost access to far more information than has been gained from the collection of communications from new and emerging technologies. Deliberately modifying their products to avoid compliance with court orders makes it appear as though the private sector has usurped Congressional and judicial authorities.[457] This may have been a calculated decision on the part of Apple and Google, gambling that it will be quite some time before legislators are able to agree on a solution, as many less controversial bills are stalled or voted down in Congress. Meanwhile, these corporations may continue reaping marketing benefits, as well as expending fewer resources assisting law enforcement.

The third conclusion is that prosecutors may inadvertently be doing the agencies they represent and law enforcement in general a disservice regarding the wiretap statistics

---

[454] Hibbard, "Wiretapping the Internet," 376, 390.

[455] H.R., *Encryption Tightrope*, 52.

[456] Ibid.

[457] Ibid., 56, 132, 160, 174; "Inside the FBI: Director Comey Addresses Cyber Security Experts," Federal Bureau of Investigation, September 2, 2016, https://www.fbi.gov/audio-repository/inside-podcast-comey-cyber-speech-090216.mp3/view.

reported to the court. Prosecutors in some cases choose to delay reporting these statistics to protect ongoing investigations, but this data is eventually reported to the court when the investigation concludes.[458] The problem lies in the statistics that remain unreported. The reported statistics are passed on to Congress who evaluates them for various purposes, to include assessing the seriousness of the encryption issue.[459] When roughly one-third of the statistics are not reported in a timely manner, or at all, this may prove detrimental to garnering support to address the encryption problem.[460]

The fourth conclusion is that despite protestations by privacy and security experts, it is possible to provide law enforcement with the access to communications it requires, while minimizing the risk to individual privacy and corporate intellectual property. Apple deployed their enhanced encryption following the Edward Snowden leaks.[461] However, the company admits that to their knowledge, their previous encryption and code had not been undermined.[462] This level of encryption provided adequate privacy protections, yet remained accessible to law enforcement with Apple's assistance.[463]

The final conclusion is that out of the six decryption/access techniques analyzed, the two that show the most promise are: split-key encryption and the insertion of spyware also known as a State Trojan.[464] Employment of either option would require new or amended legislation. The stalemate that Congress has been experiencing makes passing or amending such controversial legislation a significant challenge.

When split-key encryption is employed, two or more entities collaborate to decrypt the data.[465] The advantages of this method are decreased vulnerability to outside

---

[458] United States Courts, "FAQs: Wiretap Reports."

[459] Ibid.

[460] Ibid.

[461] Hennessey and Wittes, "Apple Is Selling You an iPhone"; Timberg, "Newest Androids."

[462] H.R., *Encryption Tightrope*, 190.

[463] District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 13.

[464] Schaul, "Encryption Techniques"; *Homeland Security Newswire*, "Growing Opposition in Germany."

[465] Ibid.

hackers or internal bad actors, data integrity protection, secure enough to withstand judicial scrutiny during court proceedings, and absorption of costs by the private sector, which would benefit state and local law enforcement agencies whose budgets are often constrained.[466] The disadvantages to the split-key option would be the need for new or amended legislation to compel device designers or communication providers to maintain the capability to access content, regardless of how sophisticated the encryption becomes. This option also requires the assistance of the private sector, whose willingness to assist law enforcement has waned since 2014.[467] Additionally, the government must pay device designers and communication providers for costs incurred for providing assistance, and response times vary depending on the provider.[468] The private sector also has the resources to lobby Congress on its behalf, potentially stalling or derailing proposed legislation.[469] Legislative effectiveness and private sector cooperation present considerable hurdles that must be overcome if this option is employed.

The second option that has potential is the insertion of spyware onto a target device by law enforcement. Germany passed legislation in June 2017 granting police agencies the authority to use this technique.[470] The insertion of spyware allows law enforcement to view communications prior to encryption or after decryption has occurred.[471] The advantages to this option are the ease and anticipated low costs of spyware insertion, faster receipt of required data due to discontinued reliance on device designers or communication providers, and not having to compete with future encryption techniques, which could result in additional cost and time savings. Additionally, individual privacy and corporate intellectual property are protected as the spyware is inserted onto a specific device, contingent upon a judicially approved court order. The

---

[466] Schaul, "Encryption Techniques"; *Homeland Security Newswire*, "Growing Opposition in Germany"; District Attorney, New York County, *Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety: An Update*, 16, 30; Hibbard, "Wiretapping the Internet," 390; Peterson and Nakashima, "Obama Administration Explored Ways to Bypass Smartphone Encryption."

[467] Hennessey and Wittes, "Apple Is Selling You an iPhone."

[468] CBS News, "Verizon, AT&T Get Most."

[469] Shaban, "Facebook and Apple Spent More on Lobbying."

[470] *Homeland Security Newswire*, "Growing Opposition in Germany."

[471] German Bundestag, "18 Election Period 12785," 49.

disadvantages of this option lie mostly in the fact that it is untested. Currently, it is unknown how this method would withstand judicial scrutiny in court proceedings, how difficult it is to extract the data in a manner that meets the threshold for preserving evidence, what training will be required or how long it will take to become proficient for those tasked with intercepting communications via this method, or if the user/target notices a difference in device performance that would alert him/her to law enforcement's actions. An additional disadvantage is the necessity for new legislation granting law enforcement the authority to insert spyware, contingent on judicial approval. However, as the private sector is not being required to modify their product or asked to absorb related costs, any lobbying efforts on their behalf may not be as effective, which could ease passage of legislation. The introduction of any new law enforcement methods come with risks, but given law enforcement's current predicament in accessing encrypted communications, the advantages to spyware insertion seem to outweigh the disadvantages, as shown in Table 4.

Table 4. Advantages and Disadvantages of Split-Key Encryption versus Spyware

	Split-Key Encryption	**Spyware/State Trojan**
Advantages ✓ Disadvantages ✓		
Costs:		
Low Cost to Law Enforcement		✓
No Costs to Private Sector		✓
Engineering Costs Borne by Private Sector	✓	
Private Sector Interception Fees	✓	
Court Proceedings:		
Withstand Judicial Scrutiny	✓	
May Not Withstand Judicial Scrutiny		✓
Data Integrity/Evidence:		
Data Integrity Protected	✓	
Questionable Evidence Preservation		✓
Hacking/Insider Threat:		
Decreased Outside Hacker Vulnerability	✓	✓

	Split-Key Encryption	Spyware/State Trojan
Advantages ✓ Disadvantages ✓		
Decreased Insider Risk	✓	
Specific to One Device – Does Not Endanger All Users		✓
Protects Intellectual Property	✓	✓
Legislation:		
New Legislation Required	✓	✓
Private Sector:		
Faster Receipt of Data		✓
No Competition with Future Encryption		✓
No Reliance on Private Sector		✓
Private Sector Lobby Less Effective		✓
Private Sector Lobby	✓	
Private Sector Response Time	✓	
Private Sector Willingness to Comply	✓	
Misc.:		
Ease of Use		✓
Training/Learning Curve		✓
Unknown if Seamless to Target		✓
Untested		✓

Totals:		
	Split-Key Encryption	**Spyware/State Trojan**
Advantages	**6**	**10**
Disadvantages	**5**	**6**

What Table 4 demonstrates is that both decryption/access options have advantages and disadvantages. Access to communications and device content is a complex issue. Perhaps the reason it has been so difficult to overcome is that it has traditionally been approached as a single issue, when in reality it requires a two-pronged approach. When law enforcement has the device in its custody, subsequent to an arrest, search warrant or court order, the focus will likely be on retrieving data at rest. Data at rest refers to all content stored on the device, not ongoing communications in real

time.[472] In these instances, split-key encryption seems to be the best option for fulfilling law enforcement's needs while still providing a level of security for individual privacy and corporate intellectual property. As this option relies on the private sector's assistance, it would likely preserve the integrity of the data, withstand judicial scrutiny and keep governmental costs down.

Conversely, surreptitious monitoring of data in motion, communications occurring in real time, is a valuable tool used by law enforcement engaged in ongoing, long-term investigations. In these instances, the device remains in the hands of the subject, who is unaware of the electronic surveillance.[473] The installation of a State Trojan/spyware may be the most efficient method for law enforcement to monitor communications without having to rely on the private sector for assistance. Although spyware insertion is to date an untested method or at least not widely reported via open sources, it seems to have many advantages. The appropriate response to emerging communication platforms and enhanced encryption by law enforcement and legislators should include innovative techniques, and the insertion of spyware onto a target's device is certainly revolutionary. Therefore, drafting legislation that addresses how law enforcement can obtain both data at rest and data in motion, using the techniques described above may provide the solutions necessary for these issues.

[472] Nate Lord, "Data Protection: Data in Transit vs. Data at Rest," *Digital Guardian* (blog), June 13, 2016, https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.

[473] Ibid.

APPENDIX

WT-2A Federal
(Rev. 08/2015)

Administrative Office of the United States Courts

Part 1 (Judge's Report - Federal)
Report of Application and/or Order Authorizing Interception of Communications
(To be reported by January 31 for denied applications and for approved applications for orders that expired during the preceding year, pursuant to 18 U.S.C. § 2519(1))

1. Judge Authorizing or Denying the Application

Judge's First Name:	Middle Initial:	Last Name:	Suffix:

Court Jurisdiction: Select:	Court Reference No.:

2. Source - Official Making Application

Official's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Title: *(i.e., DA, etc.)* Select or enter a title:	Official's Jurisdiction/Agency:

3. Deputy Assistant Attorney General (DAAG)

Deputy Assistant Attorney General's Name Select:	Other Deputy Assistant Attorney General's Name

3A. Prosecution Official Authorizing Application

Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:

Prosecutor's Jurisdiction: Select:	Prosecutor Reference No.:

3B. Law Enforcement Agency Conducting the Wiretap

Agency Name *(FBI, DEA, etc.)* Select or enter an Agency Name:	Agency Reference No.:

Contact Person's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:	Extension:

4. Offense *(Most Serious)*	**5. Type of Order** *(Select One)*
Most Serious Offense: Select:	☐ Ordinary Specification Order *(including most cell phone wiretaps)*
Title/Section of Offense:	☐ Roving - Relaxed Specification Order Granted under 18 U.S.C. 2518(11)

6. Duration of Intercept

Order or Extension	No. of Days	Date of Application	*Check One* Denied	*Check One* Granted	Date Order Denied or Granted	Date that a Granted Order/Extension was Modified or Amended, if applicable.
Original Request			☐	☐		Date Modified /Amended
1st Extension			☐	☐		Date Modified /Amended
2nd Extension			☐	☐		Date Modified /Amended
3rd Extension			☐	☐		Date Modified /Amended
4th Extension			☐	☐		Date Modified /Amended
5th Extension			☐	☐		Date Modified /Amended
6th Extension			☐	☐		Date Modified /Amended
Use the last page of the form for additional extensions.	**Total Number of Extensions:** 0				**Total Days Authorized:** 0	

Page 1

WT-2A Federal
(Rev. 08/2015)

7. Type of Intercept *(Check all that apply to this order/authorization)*

Phone - check device(s)	**Oral -** check device(s)	**Electronic -** check device(s)
☐ Cellular or Mobile Telephone	☐ Microphone / Eavesdrop	☐ Computer *(including email)*
☐ Standard Telephone *(land line)*	☐ Other *(specify)*	☐ Digital Pager
☐ Other *(specify)*		☐ Fax Machine
		☐ Text Messaging
		☐ App
		☐ Other *(specify)*

8. Location Shown in Intercept Order *(Check all that apply to this order/authorization)*

☐ Portable Device - Carried by/on Individual *(e.g., cell phone, pager)*
☐ Personal Residence *(e.g., single family house, apartment, mobile home, rooming house, dormitory)*
☐ Business *(e.g., store, office, restaurant, gym, hospital, school)*
☐ Public Area *(e.g., pay telephone, park, station, airport, library, street, cemetery)*
☐ Other Location *(e.g., motel, prison, jail, vehicle, another specified location not listed)*
Specify
☐ No Location Specified in Order *(either "roving" as shown in item 5, or other circumstances)*
Describe

8A. Judge's Signature *(Use /s/ or Check Endorsement Box)*

	☐ Judge's Endorsement	Date:	Telephone No.:

8B. Report Prepared By

Report Preparer's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:	Extension:

Title:	Date:

Instructions

When Part 1 (Judge's Report) is completed, do the following:

(1) Click the "Validate Part 1" button to identify any data quality issues with Part 1.
(2) Save a PDF copy of the completed form by clicking the "Save As" button below and assigning a unique file name.
(3) Click the "Submit by Email" button below to submit this form or attach one or more saved PDF forms to an email and send to SD-WIRETAP@AO.USCOURTS.GOV.
(4) Provide an electronic copy of the completed Part 1 to the official making the application.
(5) Retain a copy of the completed Part 1 for the judge's files.

Additional Instruction

Judges stop here. Prosecutors and Law Enforcement Agencies continue to Part 2 of the WT-2 Form.

Validate Part 1 | Save As | Submit by Email

WT-2A Federal
(Rev. 08/2015)

Administrative Office of the United States Courts

Part 2 (Prosecutor's Report - Federal)
Report of Application and/or Order Authorizing Interception of Communications

(To be reported by March 31 for terminated investigations, pursuant to 18 U.S.C. § 2519(2))

Judge Authorizing or Denying the Application

Judge's First Name:	Middle Initial:	Last Name:	Suffix:
Court Jurisdiction:		Court Reference No.:	

Prosecution Official Authorizing Application

Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:	Telephone No.:
Prosecutor Reference No.:	Agency Reference No.:		Application Date (Original Request):	

NOTE: Items listed above should match information entered in Part 1 of Form WT-2.

9. Installation

☐ Never Installed ☐ Installed but Not Used ☐ Installed and Used

10. Description of Intercepts

10A. Termination Date of Interception	10B. No. of Days in Actual Use	10C. No. of Communications Intercepted ☐ Unknown	10D. No. of Persons Whose Comm. Were Intercepted ☐ Unknown	10E. No. of Incriminating Comm. Intercepted ☐ Unknown

10F. Was Encryption Encountered in this Wiretap? ☐ Yes ☐ No	10G. If Yes, Did Encryption Prevent Law Enforcement from Obtaining the Plain Text of Communications Intercepted? ☐ Yes ☐ No

11. Cost (Rounded to Nearest Dollar)

Check the option that applies:

☐ Costs for this wiretap are reported below.

☐ Costs for this wiretap are included on another wiretap form with the following reference number.

Reference Number Type: Reference Number:

☐ Costs for this wiretap are unknown at this time.

11A. Nature and Quantity of Personnel Used to Install, Monitor, and Prepare Transcripts

11B. Personnel Cost		11C. Resource Cost (installation fees, supplies, equipment, etc.)		11D. Total Cost = Personnel Cost + Resource Cost
$	+	$	=	$

12. Results

Check the option that applies:

☐ Results for this wiretap are reported below.

☐ Results for this wiretap are included on another wiretap form with the following reference number.

Reference Number Type: Reference Number:

☐ Results for this wiretap are not known at this time. *(Future results should be reported on the WT-3 Supplementary Report)*

12A1. No. of Persons Arrested	12A2. Arrest Offense (Most Serious):		12B. No. of Motions to Suppress: Granted	Denied	Pending
12C. No. of Persons Convicted	12D. No. of Trials Completed	12E. Conviction Offense (Most Serious):	12F. Title/Section of Conviction Offense:		

13. Comments and Assessment
Describe importance of the interceptions, drugs and money seizure amounts, impact on community, etc. **DO NOT** include target's name, address, phone numbers, name of gangs, or other sensitive information.

13A. Report Prepared By				
Prosecutor Responsible for Part 2	Prosecutor's First Name:	Middle Initial:	Last Name:	Suffix:
Report Preparer	☐ Check if Prosecutor and Report Preparer are the same person.			
	Report Preparer's First Name:	Middle Initial:	Last Name:	Suffix:
	Title:		Telephone No.: Extension:	Date:

Instructions

When Part 2 (Prosecutor's Report) is completed, do the following:

(1) Click the "Validate Part 2" button to identify any data quality issues with Part 2.
(2) Save a PDF copy of the completed form by clicking the "Save As" button below and assigning a unique file name.
(3) Attach one or more saved PDF forms to an email and send to the Federal Law Enforcement Agency Contact who will review and submit the PDF forms to the DOJ's Office of Enforcement Operations.
(4) Retain a copy of the completed form for your files.

Validate Part 2 Only | Validate Parts 1 & 2 | Save As

WT-2A Federal
(Rev. 08/2015)

6. Duration of Intercept *(Additional Extensions)*						
Order or Extension	No. of Days	Date of Application	*Check One* Denied	Granted	Date Order Denied or Granted	Date that a Granted Order/Extension was Modified or Amended, if applicable.
7th Extension			☐	☐		Date Modified /Amended
8th Extension			☐	☐		Date Modified /Amended
9th Extension			☐	☐		Date Modified /Amended
10th Extension			☐	☐		Date Modified /Amended
11th Extension			☐	☐		Date Modified /Amended
12th Extension			☐	☐		Date Modified /Amended
13th Extension			☐	☐		Date Modified /Amended
14th Extension			☐	☐		Date Modified /Amended
15th Extension			☐	☐		Date Modified /Amended
16th Extension			☐	☐		Date Modified /Amended
17th Extension			☐	☐		Date Modified /Amended
18th Extension			☐	☐		Date Modified /Amended
19th Extension			☐	☐		Date Modified /Amended
20th Extension			☐	☐		Date Modified /Amended
21st Extension			☐	☐		Date Modified /Amended
22nd Extension			☐	☐		Date Modified /Amended
23rd Extension			☐	☐		Date Modified /Amended
24th Extension			☐	☐		Date Modified /Amended
25th Extension			☐	☐		Date Modified /Amended
26th Extension			☐	☐		Date Modified /Amended
27th Extension			☐	☐		Date Modified /Amended
28th Extension			☐	☐		Date Modified /Amended
29th Extension			☐	☐		Date Modified /Amended
30th Extension			☐	☐		Date Modified /Amended
31st Extension			☐	☐		Date Modified /Amended
32nd Extension			☐	☐		Date Modified /Amended
33rd Extension			☐	☐		Date Modified /Amended
34th Extension			☐	☐		Date Modified /Amended
35th Extension			☐	☐		Date Modified /Amended
36th Extension			☐	☐		Date Modified /Amended

Page 5

Figure 2. WT-2A Federal Form—Report of Application and/or Order Authorizing Interception of Communications[474]

[474] Source: United States Courts, "Wiretap Reports."

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, and John Gilmore et al. *Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*. Cambridge, MA: MIT Computer Science & Artificial Intelligence Lab, 2015. https://people.csail.mit.edu/rivest/pubs/AABBx15x.pdf.

Administrative Office of the United States Courts. *WT-2A Federal Form*. Washington, DC: Administrative Office of the United States Courts, 2015. http://www.uscourts.gov/sites/default/files/form_wt-2a_0.pdf.

Anonymous. "Apple's Privacy Headache Intensifies." *Information Management* 47, no. 4 (August 2013): 18.

Apple. *Legal Process Guidelines, Government and Law Enforcement within the United States*. Cupertino, CA: Apple, 2017. https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf.

———. *iOS Security*. Cupertino, CA: Apple, 2017. https://images.apple.com/business/docs/iOS_Security_Guide.pdf.

Apple Support. "If You Forgot the Passcode for Your iPhone, iPad, or iPod Touch, or Your Device Is Disabled." December 18, 2017. https://support.apple.com/en-us/HT204306.

Arbus, Melissa. "A Legal U-Turn: The Rehnquist Court Changes Direction and Steers Back to the Privacy Norms of the Warren Era." *Virginia Law Review* 89, no. 7 (November 2003): 1729–1777.

Bankston, Kevin. "It's Time to End the 'Debate' on Encryption Backdoors." Just Security, July 7, 2015. https://www.justsecurity.org/24483/end-debate-encryption-backdoors/.

Bardach, Eugene, and Eric M. Patashnik. *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving*. Thousand Oaks, CA: CQ Press an Imprint of SAGE Publications, Inc., 2016. Kindle.

Bartow, Ann. "A Feeling of Unease about Privacy Law." University of New Hampshire—School of Law. January 1, 2006. http://scholars.unh.edu/cgi/viewcontent.cgi?article=1119&context=law_facpub.

Berkman Center for Internet & Society at Harvard University. *Don't Panic Making Progress on the Going Dark Debate*. Cambridge, MA: Berkman Center for Internet & Society at Harvard University, 2016. https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Bleiker, Carla. "New Surveillance Law: German Police Allowed to Hack Smartphones." Deutsche Welle, June 22, 2017. http://www.dw.com/en/new-surveillance-law-german-police-allowed-to-hack-smartphones/a-39372085.

Brantly, Aaron. "Banning Encryption to Stop Terrorists: A Worse than Futile Exercise." *CTC Sentinel*, August 2017.

Bright, Peter. "Encryption Isn't at Stake, The FBI Knows Apple Already Has the Desired Key." Ars Technica, February 18, 2016. https://arstechnica.com/apple/2016/02/encrypttion-isnt-at-stake-the-fbi-knows-apple-already-has-the-desired-key/.

Cameron, Joel D. "Stasi, East German Government." *Encyclopaedia Britannica*, April 11, 2016. https://www.britannica.com/topic/Stasi.

CBS News. "Verizon, AT&T Get Most Bucks from Feds for Wiretaps." July 11, 2013. https://www.cbsnews.com/news/verizon-att-get-most-bucks-from-feds-for-wiretaps/.

Chase, Jefferson. "Things to Know about Germany's Recent Surveillance Laws." Deutsche Welle, June 26, 2017. http://www.dw.com/en/things-to-know-about-germanys-recent-surveillance-laws/a-39421060.

Cheng, Wesley. *A Practitioner's Guide to Wiretaps in Public Corruption Investigations.* New York City: Center for the Advancement of Public Integrity, Columbia Law School, 2016. http://www.law.columbia.edu/sites/default/files/microsites/public-integrity/files/a_pracititioners_guide_to_wiretaps_in_public_corruption_investigations_7.25.2016_0.pdf.

Chertoff, Michael, Mike McConnell, and William Lynn. "Why the Fear Over Ubiquitous Data Encryption Is Overblown." *Washington Post*, July 28, 2015. https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html?utm_term=.fae580e2b4c7.

Cook, Tim. "A Message to Our Customers." Apple, February 16, 2016. https://www.apple.com/customer-letter/.

Crowley, Michael G., and Michael N. Johnstone. "Protecting Corporate Intellectual Property: Legal and Technical Approaches." *Business Horizons* 59, no. 6 (December 2016): 623–633.

Cryptography World. “Key Management: A Cryptography Tutorial.” Accessed January 23, 2017. http://www.cryptographyworld.com/key.htm.

District Attorney, New York County. *Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety*. Manhattan, NY: District Attorney, New York County, 2015. http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

———. *Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety: An Update to the November 2015 Report*. Manhattan, NY: District Attorney, New York County, 2016. http://manhattanda.org/sites/default/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf.

Essers, Loek. “Apple’s Privacy Policy Violates German Data Protection Law, Berlin Court Rules.” Computerworld, May 7, 2013. http://www.computerworld.com/article/2497084/data-center/apple-s-privacy-policy-violates-german-data-protection-law--berlin-court-rules.html.

Etzioni, Amitai. “Apple: Good Business, Poor Citizen?” *Journal of Business Ethics*, May 31, 2016. doi: 10.1007/s10551-016-3233-4.

Federal Bureau of Investigation. “Counterterrorism, Counterintelligence, and the Challenges of Going Dark.” July 8, 2015. https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark.

———. “Encryption and Cyber Security for Mobile Electronic Communication Devices.” April 29, 2015. https://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.

———. “Inside the FBI: Director Comey Addresses Cyber Security Experts.” September 2, 2016. https://www.fbi.gov/audio-repository/inside-podcast-comey-cyber-speech-090216.mp3/view.

Federal Communications Commission. “Communications Assistance for Law Enforcement Act.” February 10, 2011. https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

———. “Voice over Internet Protocol (VoIP).” November 18, 2010. https://www.fcc.gov/general/voice-over-internet-protocol-voip.

Finklea, Kristin. *Encryption and Evolving Technology: Implications for U.S. Law Enforcement Investigations*. CRS Report No. R44187. Washington, DC: Congressional Research Service, 2016. https://fas.org/sgp/crs/misc/R44187.

Finklea, Kristin, Richard M. Thompson II, and Chris Jaikaran. *Court-Ordered Access to Smart Phones: In Brief*. CRS Report No. R44396. Washington, DC: Congressional Research Service, 2016. https://fas.org/sgp/crs/misc/R44396.pdf.

Fox-Brewster, Thomas. "Forget About Backdoors, This Is the Data WhatsApp Actually Hands to Cops." Forbes, January 22, 2017. http://www.forbes.com/sites/Thomas brewster/2017/01/22/whatsapp-facebook-backdoor-government-data-request/.

———. "SiriusXM Satellite Radio Tech Turned into Surveillance Device." Forbes, January 15, 2017. https://www.documentcloud.org/documents/3295672-Sirius XM-Satellite-Radio-Tech-Turned-Into.html.

Friedersdorf, Conor. "Is Law Enforcement Crying Wolf about the Dangers of Locked Phones?" *Atlantic*, February 19, 2016. https://www.theatlantic.com/politics/ar chive/2016/02/is-law-enforcement-crying-wolf-about-the-dangers-of-locked-phones/470055/.

Gellman, Barton, and Laura Poitras. "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." *Washington Post*, June 7, 2013. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a 0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.b263741a8ae2.

German Bundestag. "18 Election Period 12785." June 20, 2017. https://translate.google. com/translate?hl=en&sl=de&u=http://dip21.bundestag.de/dip21/btd/18/127/1812 785.pdf&prev=search.

———. "Stenograph Record, 240th Session, Plenary 18/240." June 22, 2017.

Greenberg, Andy. "Hacker Lexicon: What Is End-to-End Encryption?" Wired, November 25, 2014. https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

Greenblatt, Mark, and Robert Cribb. "Encrypted Evidence Is Increasingly Hampering Criminal Investigations, Police Say." November 6, 2015. http://www.wcpo.com/ news/national/encrypted-evidence-is-increasingly-hampering-criminal-investiga tions-police-say?page=2.

Greenwald, Glenn, and Ewen MacAskill. "NSA Prism Program Taps into User Data of Apple, Google and Others." *Guardian*, June 7, 2013. https://www.theguardian. com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20trail:Network%20front%20-%20special%20tra il:Position1.

Gross, Grant. "Judge: Give NSA Unlimited Access to Digital Data." PCWorld, December 4, 2014. http://www.pcworld.com/article/2855776/judge-give-nsa-unlimited-access-to-digital-data.html.

Hattersley, Lucy. “How to Stop iPhone From Asking to Update to the Latest Version.” Macworld UK, July 6, 2016. http://www.macworld.co.uk/how-to/iphone/how-stop-ios-nagging-you-update-latest-version-3641478/.

Hellmuth, Dorle. “Countering Jihadi Terrorists and Radicals the French Way.” *Studies in Conflict and Terrorism*, August 24, 2015. http://www.tandfonline.com/loi/uter20.

Hennessey, Susan, and Benjamin Wittes. “Apple Is Selling You a Phone, Not Civil Liberties.” *Lawfare* (blog), February 18, 2016. https://www.lawfareblog.com/apple-selling-you-phone-not-civil-liberties.

Hibbard, Christa M. “Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance.” *Federal Communications Journal* 64, no. 2, art 5 (2012): 371–399. http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1617&context=fclj.

Homeland Security Newswire. “Growing Opposition in Germany to New Surveillance Measures.” June 26, 2017. http://www.homelandsecuritynewswire.com/dr20170626-growing-opposition-in-germany-to-new-surveillance-measures.

House Judiciary Committee & House Energy and Commerce Committee. *Encryption Working Group Year End Report*. Washington, DC: House Judiciary Committee & House Energy and Commerce Committee, 2016. http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/documents/114/analysis/20161219EWGFINALReport_0.pdf.

Hume, David. *An Enquiry Concerning the Principles of Morals*. Salt Lake City, UT: Project Gutenberg, 2010; 1912 reprint of the edition of 1777. https://www.gutenberg.org/files/4320/4320-h/4320-h.htm.

Iyengar, Rishi. “Apple Is Removing VPN Apps that Allow Users to Skirt China’s Great Firewall.” CNN Money, July 29, 2017. http://money.cnn.com/2017/07/29/technology/china-apple-app-store-vpn-express/index.html.

Jagadish, Hosagrahar Visvesvaraya. “Passwords, Privacy and Protection: Can Apple Meet FBI’s Demand without Creating a ‘Backdoor’?” *Scientific Computing*, February 24, 2016. http://search.proquest.com.libproxy.nps.edu/docview/1777528493/abstract/E615D3E0B2B0447APQ/6.

Kelly, Heather. “OMG, The Text Message Turns 20. But Has SMS Peaked?” CNN, December 12, 2012. http://www.cnn.com/2012/12/03/tech/mobile/sms-text-message-20/index.html.

Khawaja, Irfan. “Not a Suicide Pact: The Constitution in a Time of National Emergency.” *Dissent Magazine*, 2006. https://www.dissentmagazine.org/wp-content/files_mf/1389818084d8Khawaja.pdf.

Knobloch, Carley. “11 Reasons We Love Amazon Alexa (And Why You Should Buy One Right Now).” Today, December 27, 2017. https://www.today.com/home/best-amazon-alexa-skills-echo-dot-show-t115489.

Landau, Susan. “The Real Security Issues of the iPhone Case, Law Enforcement Needs 21st-Century Investigative Savvy.” *Science* 352, no. 6292 (June 17, 2016): 1398–9.

Lectric Law Library. “Legal Definition of Privileged Communication.” Accessed June 16, 2017. http://www.lectlaw.com/def2/p084.htm.

Legal Information Institute, Cornell University Law School. “Commerce Clause.” July 3, 2008. https://www.law.cornell.edu/wex/commerce_clause.

———. “Fourth Amendment.” February 5, 2010. https://www.law.cornell.edu/constitution/fourth_amendment.

Longtin, Robert. “Apple, the FBI, and an Act from 1789: The FBI’s Impermissible Use of the All Writs Act.” *Columbia Business Law Review*, March 28, 2016. https://cblr.columbia.edu/apple-the-fbi-and-an-act-from-1789-the-fbis-impermissible-use-of-the-all-writs-act/.https://cblr.columbia.edu/apple-the-fbi-and-an-act-from-1789-the-fbis-impermissible-use-of-the-all-writs-act/.

Lord, Nate. “Data Protection: Data in Transit vs. Data at Rest.” *Digital Guardian* (blog), June 13, 2016. https://digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest.

Mansfield-Devine, Steve. “The Battle for Privacy.” *Network Security*, June 2016.

Martin, Rachel. “It’s Not Just the iPhone Law Enforcement Wants to Unlock.” NPR, February 21, 2016. http://www.npr.org/2016/02/21/467547180/it-s-not-just-the-iphone-law-enforcement-wants-to-unlock.

Meyer, David. “Will Apple’s iOS 11 ‘Cop Button’ Help Protect iPhone Privacy?” *Fortune*, August 17, 2017. http://fortune.com/2017/08/18/apple-ios-11-cop-button-iphone-ipad-privacy/.

Microsoft Developer Network. “Asymmetric Keys (Windows).” Accessed February 5, 2017. https://msdn.microsoft.com/en-us/library/windows/desktop/aa387460(v=vs.85).aspx.

Microsoft Support. “Description of Symmetric and Asymmetric Encryption.” Accessed February 5, 2017. https://support.microsoft.com/en-us/help/246071/description-of-symmetric-and-asymmetric-encryption.

Mullender, Richard. “Not a Suicide Pact: The Constitution in a Time of Emergency.” *Journal of Law and Society* 35, no. 3 (2008): 422–427.

Mulligan, Deirdre, and Nick Doty. “Design Wars: The FBI, Apple and Hundreds of Millions of Phones.” *UC Berkeley* (blog), March 3, 2016. http://blogs.berkeley.edu/2016/03/03/design-wars-the-fbi-apple-and-hundreds-of-millions-of-phones-3/.

Newsweek. “Timeline of Recent Terror Attacks in Western Europe.” April 8, 2017. http://www.newsweek.com/timeline-recent-terror-attacks-western-europe-580977.

Pagliery, Jose. “Apple Promises Privacy—But Not On iCloud.” CNN Money, February 22, 2016. http://money.cnn.com/2016/02/22/technology/apple-privacy-icloud/index.html.

“Personal Data Encryption.” *Congressional Digest* 95, no. 6 (June 2016).

Perlroth, Nicole. “Security Experts Oppose Government Access to Encrypted Communication.” *New York Times*, July 7, 2015. http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html.

Peterson, Andrea, and Ellen Nakashima. “Obama Administration Explored Ways to Bypass Smartphone Encryption.” *Washington Post*, September 24, 2015. https://www.washingtonpost.com/world/national-security/obama-administration-ponders-how-to-seek-access-to-encrypted-data/2015/09/23/107a811c-5b22-11e5-b38e-06883aacba64_story.html.

Pew Research Center for the People and the Press. “More Support for Justice Department than for Apple in Dispute over Unlocking iPhone.” February 22, 2016. http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/.

Phys Org. “Germany Expands Surveillance of Encrypted Message Services.” June 22, 2017. https://phys.org/news/2017-06-germany-surveillance-encrypted-message.html.

Posner, Richard A. “The Right of Privacy.” University of Chicago Law School, Chicago Unbound, 1977. http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2803&context=journal_articles.

Potapchuk, John L. “A Second Bite at the Apple: Federal Courts’ Authority to Compel Technical Assistance to Government Agents in Accessing Encrypted Smartphone Data under the All Writs Act.” *Boston College Law Review* 57, no. 4 (2016): 1403–46.

Rayome, Alison DeNisco. “Police Can Force You to Give up Your iPhone Password, Florida Court Rules.” TechRepublic, December 20, 2016. http://www.techrepublic.com/article/police-can-force-you-to-give-up-your-iphone-password-florida-court-rules/.

RT News. “Thousands of Germans Rally to End Government Spying.” August 31, 2014. https://www.rt.com/news/184000-berlin-protests-surveillance-government/.

Savage, Charlie. “U.S. Tries to Make It Easier to Wiretap the Internet.” *New York Times*, September 27, 2010. http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=3&hpw&.

Schaul, Kevin. “Encryption Techniques and the Access They Give.” *Washington Post*, April 10, 2015. https://www.washingtonpost.com/apps/g/page/world/encryption-techniques-and-access-they-give/1665/.

Schlabach, Gabriel R. “Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act.” *Stanford Law Review* 67, no. 3 (March 2015): 677–721.

Schneier, Bruce. “Essays: The Eternal Value of Privacy.” Schneier on Security, May 18, 2006. https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html.

Shaban, Hamza. “At the Start of the Trump Era Facebook and Apple Spent More on Lobbying than Ever.” CNBC, April 21, 2017. https://www.cnbc.com/2017/04/21/at-the-start-of-the-trump-era-facebook-and-apple-spent-more-on-lobbying-than-ever.html.

Solove, Daniel J. “I’ve Got Nothing to Hide and Other Misunderstandings of Privacy.” 2007. http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications.

Swire, Peter, and Joshua Oliver. “The Golden Age of Surveillance.” Slate, July 15, 2015. http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html.

Taylor, Guy. “Hezbollah Moving ‘Tons of Cocaine’ in Latin America, Europe to Finance Terror Operations.” *Washington Times*, June 8, 2016. http://www.washingtontimes.com/news/2016/jun/8/hezbollah-moving-tons-of-cocaine-in-latin-america-/.

Thomas, Lauren. “Amazon’s Echo Dot Has Record Holiday Weekend, Millions of Devices Sold.” CNBC, November 28, 2017. https://www.cnbc.com/2017/11/28/amazons-echo-dot-has-record-holiday-weekend-millions-of-devices-sold.html.

Timberg, Craig. “Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police.” *Washington Post*, September 18, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/?utm_term=.7afa491b5834.

U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance. “Electronic Communications Privacy Act of 1986, Justice Information Sharing.” July 30, 2013. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.

———. “Title III of the Omnibus Crime Control and Safe Streets Act of 1968.” September 9, 2013. https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284.

United Nations Office on Drugs and Crime. “Drug Trafficking and the Financing of Terrorism.” Accessed June 16, 2017. http://www.unodc.org/unodc/en/frontpage/drug-trafficking-and-the-financing-of-terrorism.html.

United States Courts. “FAQs: Wiretap Reports.” Accessed August 21, 2017. http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports/faqs-wiretap-reports.

———. “Wiretap Reports.” Accessed May 10, 2017. http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

Washington Post. “Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants.” September 18, 2014. https://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html?utm_term=.0192bb7759ae.

Wu, Felix. “No Easy Answers in the Fight over iPhone Decryption.” *Communications of the ACM* 59, no. 9 (September 2016): 20–22.

Zetter, Kim. “Hacker Lexicon: What Is Full Disk Encryption?” Wired, July 2, 2016. https://www.wired.com/2016/07/hacker-lexicon-full-disk-encryption/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California